RELEASE 8.2

Infoblox NIOS Administrator Guide
| 1.4.7.10 Backing Up and Restoring Configuration Files | 359 |
| 1.4.7.11 Using Database Snapshots | 363 |
| 1.4.7.12 Downloading Support Bundles | 364 |
| 1.4.8 Chapter 11 bloxTools Environment | 364 |
| 1.4.8.1 About the bloxTools Environment | 365 |
| 1.4.8.2 Using the bloxTools Environment | 366 |
| 1.4.8.3 Monitoring the Service | 368 |
| 1.4.9 Chapter 12 RIR Registration Updates | 368 |
| 1.4.9.1 About the RIPE Database | 369 |
| 1.4.9.2 Requirements and Permissions | 369 |
| 1.4.9.3 Configuring RIR Registration Updates | 369 |
| 1.4.9.4 Managing RIR Data | 370 |
| 1.4.9.5 Managing RIR Attributes | 373 |
| 1.4.9.6 Monitoring RIR Data | 376 |
| 1.5 Part 3 IP Address Management | 378 |
| 1.5.1 Chapter 13 IP Address Management | 378 |
| 1.5.1.1 About Host Records | 379 |
| 1.5.1.2 Managing IPv4 Networks | 385 |
| 1.5.1.3 Viewing and Managing IPv4 Addresses | 391 |
| 1.5.1.4 Managing IPv6 Networks | 396 |
| 1.5.1.5 Viewing IPv6 Data | 400 |
| 1.5.1.6 Managing IPv4 and IPv6 Addresses | 401 |
| 1.5.1.7 Configuring Thresholds for IPAM Utilization | 404 |
| 1.5.1.8 About Network Insight | 405 |
| 1.5.1.9 Viewing Identity Mapping Information | 405 |
| 1.5.2 Chapter 14 IP Discovery and vDiscovery | 407 |
| 1.5.2.1 IP Discovery Process | 409 |
| 1.5.2.2 Supported IP Discovery Methods | 409 |
| 1.5.2.3 Guidelines Before Starting a Discovery | 411 |
| 1.5.2.4 Configuring IP Discovery | 412 |
| 1.5.2.5 Configuring vDiscovery Jobs | 414 |
| 1.5.2.6 Viewing Discovered Data | 428 |
| 1.5.2.7 Managing Discovered Data | 430 |
| 1.5.2.8 Integrating Discovered Data From NetMRI | 434 |
| 1.5.3 Chapter 15 Infoblox Network Insight | 434 |
| 1.5.3.1 Supported Appliances for Network Insight | 436 |
| 1.5.3.2 Consolidator and Probes | 437 |
| 1.5.3.3 Deployment Guidelines for Consolidator and Probes | 438 |
| 1.5.3.4 Supported Discovery Methods | 438 |
| 1.5.3.5 Starting Discovery | 440 |
| 1.5.3.6 Managing Discovery | 441 |
| 1.5.3.7 Discovering VRF Virtual Networks | 441 |
| 1.5.3.8 Administrative Permissions for Discovery | 449 |
| 1.5.3.9 Starting and Stopping the Discovery Service | 450 |
| 1.5.3.10 Defining the Discovery Member Type | 451 |
| 1.5.3.11 Mapping Discovery Interfaces to Network Views | 451 |
| 1.5.3.12 Configuring Discovery Properties | 452 |
| 1.5.3.13 Configuring Automatic VRF Mapping | 458 |
| 1.5.3.14 Excluding IP Addresses from Discovery | 458 |
| 1.5.3.15 Discovering Devices and Networks | 459 |
| 1.5.3.16 Managing Discovered Data | 463 |
| 1.5.3.17 About Automatic Conversion Rules | 469 |
| 1.5.3.18 Viewing Discovered Devices and their Properties | 473 |
| 1.5.3.19 Accessing Detailed Device Information | 475 |
| 1.5.3.20 Viewing Discovery Status | 482 |
| 1.5.3.21 Executing Discovery Diagnostics | 484 |
| 1.5.3.22 Disabling Discovery for a Network | 484 |
| 1.5.3.23 Adding Discovery Device Support | 485 |
| 1.5.3.24 Port Control Features in Network Insight | 485 |
| 1.5.3.25 Provisioning and De-Provisioning Networks | 489 |
| 1.5.3.26 Creating Port Reservations for IPAM Objects | 492 |
| 1.5.3.27 Defining Blackout Periods | 498 |
| 1.5.3.28 Defining Port Configuration Blackout Periods | 499 |
| 1.5.3.29 Conflict Resolution in Network Insight | 501 |
| 1.5.4 Using the bloxTools Environment | 504 |
| 1.6 Part 4 DNS | 504 |
| 1.6.1 Chapter 16 Infoblox DNS Service | 504 |
| 1.6.1.1 Configuring DNS Overview | 504 |
| 1.6.1.2 About Inheriting DNS Properties | 505 |
| 1.6.1.3 Understanding DNS for IPv6 | 506 |
| 1.6.2 Chapter 17 Configuring DNS Services | 508 |
| 1.6.2.1 About Time To Live Settings | 510 |
| 1.6.2.2 Configuring Hostname and Server ID Options | 512 |
Table of Contents

1.6.2.3 Enabling and Disabling DNS Health Check Monitor ........................................................... 512
1.6.2.4 Adding an Email Address to the SOA Record ........................................................................ 513
1.6.2.5 Notifying External Secondary Servers .................................................................................... 513
1.6.2.6 Enabling the Configuration of RRSset Orders ....................................................................... 514
1.6.2.7 Specifying Port Settings for DNS ............................................................................................. 514
1.6.2.8 Specifying Static Source Ports .................................................................................................. 515
1.6.2.9 Using Extension Mechanisms for DNS (EDNS0) ................................................................. 516
1.6.2.10 Deleting PTR Records associated with A or AAAA Records .............................................. 516
1.6.2.11 Specifying Minimal Responses ............................................................................................. 516
1.6.2.12 Starting and Stopping the DNS Service ................................................................................ 517
1.6.2.13 About DNS Cache ................................................................................................................ 517
1.6.2.14 Viewing DNS Cache Entries .................................................................................................. 518
1.6.2.15 Using Forwarders .................................................................................................................... 519
1.6.2.16 Controlling DNS Queries ...................................................................................................... 520
1.6.2.17 Enabling Recursive Queries .................................................................................................. 520
1.6.2.18 Controlling AAAA Records for IPv4 Clients ........................................................................ 523
1.6.2.19 About NXDOMAIN Redirection ............................................................................................. 524
1.6.2.20 Detecting and Mitigating DNS DDoS Attacks ........................................................................ 527
1.6.2.21 Automated Mitigation of Phantom Domain Attacks ............................................................ 527
1.6.2.22 Detecting NXDOMAIN Attacks ............................................................................................ 529
1.6.2.23 Mitigating Possible NXDOMAIN Attacks ............................................................................. 532
1.6.2.24 Support for RRL (Response Rate Limiting) .......................................................................... 532
1.6.2.25 About Blacklists ..................................................................................................................... 532
1.6.2.26 Enabling Zone Transfers ........................................................................................................ 535
1.6.2.27 About Root Name Servers ..................................................................................................... 537
1.6.2.28 About Sort Lists ...................................................................................................................... 538
1.6.2.29 Configuring a DNS Blackhole List .......................................................................................... 539
1.6.2.30 Specifying Hostname Policies ............................................................................................... 540
1.6.2.31 About DNS64 .......................................................................................................................... 541
1.6.2.32 DNS Record Scavenging ......................................................................................................... 545
1.6.2.33 Monitoring DNS Queries ...................................................................................................... 549
1.6.2.34 Configuring DNS Traffic Control Properties ......................................................................... 550
1.6.3 Chapter 18 DNS Views ............................................................................................................... 550
1.6.3.1 Configuring DNS Views ........................................................................................................ 553
1.6.4 Chapter 19 Configuring DNS Zones ............................................................................................. 560
1.6.4.1 Configuring Authoritative Zones ............................................................................................ 561
1.6.4.2 Creating an Authoritative Forward-Mapping Zone ............................................................... 561
1.6.4.3 Creating an Authoritative Reverse-Mapping Zone ............................................................... 562
1.6.4.4 Creating a Root Zone ................................................................................................................. 563
1.6.4.5 Adding an Authoritative Subzone ............................................................................................ 563
1.6.4.6 Locking and Unlocking Zones .................................................................................................. 564
1.6.4.7 Enabling and Disabling Zones ................................................................................................. 564
1.6.4.8 Configuring Authoritative Zone Properties ............................................................................... 564
1.6.4.9 About DNS Integrity Check for Authoritative Zones ............................................................ 565
1.6.4.10 About Domains and Zones .................................................................................................... 566
1.6.4.11 Assigning Zone Authority to Name Servers ......................................................................... 567
1.6.4.12 Configuring Domain Controller List ..................................................................................... 571
1.6.4.13 Importing Zone Data .............................................................................................................. 572
1.6.4.14 Removing Zones ...................................................................................................................... 574
1.6.4.15 Restoring Zone Data ............................................................................................................... 576
1.6.4.16 Configuring Delegated, Forward, and Stub Zones ............................................................. 578
1.6.4.17 Viewing Zones ........................................................................................................................ 589
1.6.4.18 About Name Server Groups .................................................................................................. 589
1.6.4.19 Viewing Name Server Groups ............................................................................................... 593
1.6.5 Chapter 20 DNS Resource Records .......................................................................................... 594
1.6.5.1 SpecifyingBulk Host Name Formats ....................................................................................... 594
1.6.5.2 Adding Bulk Hosts .................................................................................................................... 596
1.6.5.3 Managing Resource Records .................................................................................................. 597
1.6.5.4 About Shared Record Groups .................................................................................................. 614
1.6.6 Chapter 21 Configuring DDNS Updates ..................................................................................... 619
1.6.6.1 Configuring DHCP for DDNS .................................................................................................. 623
1.6.6.2 Configuring DDNS Features .................................................................................................... 627
1.6.6.3 About the Client FQDN Option ............................................................................................... 629
1.6.6.4 Configuring DDNS Update Verification .................................................................................. 631
1.6.6.5 Configuring DNS Servers for DDNS ....................................................................................... 632
1.6.6.6 Supporting Active Directory .................................................................................................. 634
1.6.6.7 About GSS-TSIG ..................................................................................................................... 635
1.6.6.8 Configuring GSS-TSIG keys .................................................................................................... 647
1.6.6.9 Accepting DDNS Updates from DHCP Clients ..................................................................... 651
1.6.6.10 Accepting GSS-TSIG-Authenticated Updates ..................................................................... 652
1.6.6.11 Secure Dynamic Updates ....................................................................................................... 658
1.6.7 Chapter 22 DNSSEC .................................................................................................................. 661
Chapter 36 Managing Microsoft DHCP Services

1.7.6 Chapter 30 DHCP Failover
1.7.6.1 Failover Association Operations
1.7.6.2 Configuring Failover Associations
1.7.6.3 Managing Failover Associations

1.7.7 Chapter 31 Configuring IPv4 DHCP Filters
1.7.7.1 IP Address Allocation Using Filters
1.7.7.2 About MAC Address Filters
1.7.7.3 About Relay Agent Filters
1.7.7.4 About Option Filters
1.7.7.5 About DHCP Fingerprint Filters
1.7.7.6 Applying Filters to DHCP Objects
1.7.7.7 Managing DHCP Filters

1.7.8 Chapter 32 Authenticated DHCP
1.7.8.1 DHCP Authentication Process
1.7.8.2 Configuring DHCP Authentication
1.7.8.3 About Authentication Server Groups
1.7.8.4 About the Captive Portal
1.7.8.5 Defining the IPv4 Network and DHCP Ranges
1.7.8.6 Defining MAC Address Filters
1.7.8.7 Using the Captive Portal Wizard
1.7.8.8 About Authentication Servers
1.7.8.9 Adding and Modifying the Filters and Associations
1.7.8.10 Monitoring DHCP Authentication
1.7.8.11 Configuration Example: Configuring Authenticated DHCP
1.7.8.12 NAC Integration
1.7.8.13 Configuring NAC with RADIUS Servers
1.7.8.14 Configuring DHCP Ranges
1.7.8.15 About NAC Filters

1.7.9 Chapter 33 Managing Leases
1.7.9.1 About DHCP Leases
1.7.9.2 Viewing Current Leases
1.7.9.3 Viewing Detailed Lease Information
1.7.9.4 Viewing Lease History
1.7.9.5 Viewing Lease Event Detailed Information
1.7.9.6 Exporting Lease Records
1.7.9.7 Clearing Leases

1.8 Part 6 Managing Microsoft Windows Servers
1.8.1 Chapter 34 Managing Microsoft Windows Servers
1.8.1.1 Supported Windows Versions
1.8.1.2 Deployment Guidelines
1.8.1.3 Limitations for Scheduling Full Upgrades
1.8.1.4 Configuring Members to Manage Microsoft Servers
1.8.1.5 Configuring Grid Properties for Managing Microsoft Servers
1.8.1.6 Managing Microsoft Servers
1.8.1.7 About Active Directory Sites and Services
1.8.1.8 Configuring Active Directory Sites and Associated Networks
1.8.1.9 Managing Active Directory Sites
1.8.1.10 Managing Active Directory Sites and Associated Networks
1.8.1.11 Configuring Identity Mapping
1.8.1.12 Monitoring Managed Microsoft Servers

1.8.2 Chapter 35 Managing Microsoft DNS Services
1.8.2.1 Synchronizing DNS Data
1.8.2.2 Enabling and Disabling DNS Zone Synchronization
1.8.2.3 IDN Support for Synchronized DNS Data
1.8.2.4 Synchronizing with Multiple Servers
1.8.2.5 Managing Synchronized DNS Data
1.8.2.6 Synchronizing Updates
1.8.2.7 Viewing Members and Managed Servers
1.8.2.8 Specifying Forwarders for Microsoft Servers
1.8.2.9 Disabling and Removing Microsoft DNS Servers

1.8.3 Chapter 36 Managing Microsoft DHCP Services
1.8.3.1 Viewing Synchronized Leases
1.8.3.2 Synchronizing DHCP Failover Relationships
1.8.3.3 Synchronizing IP Addresses with Invalid MAC Addresses
1.8.3.4 Managing Synchronized DHCP Data
1.8.3.5 Managing Microsoft DHCP Servers
<table>
<thead>
<tr>
<th>1.9 Part 7 Monitoring and Reporting</th>
<th>..........................................................</th>
<th>912</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.9.1 Chapter 37 Monitoring the Appliance</td>
<td>..........................................................</td>
<td>913</td>
</tr>
<tr>
<td>1.9.1.1 Capturing DNS Queries and Responses</td>
<td>..........................................................</td>
<td>913</td>
</tr>
<tr>
<td>1.9.1.2 Enabling Grid Visualization</td>
<td>..........................................................</td>
<td>919</td>
</tr>
<tr>
<td>1.9.1.3 Grid Status</td>
<td>..........................................................</td>
<td>919</td>
</tr>
<tr>
<td>1.9.1.4 Member Status</td>
<td>..........................................................</td>
<td>919</td>
</tr>
<tr>
<td>1.9.1.5 Monitoring Services</td>
<td>..........................................................</td>
<td>923</td>
</tr>
<tr>
<td>1.9.1.6 Monitoring Tools</td>
<td>..........................................................</td>
<td>924</td>
</tr>
<tr>
<td>1.9.1.7 Tracking Object Changes in the Database</td>
<td>..........................................................</td>
<td>933</td>
</tr>
<tr>
<td>1.9.1.8 Using a Syslog Server</td>
<td>..........................................................</td>
<td>941</td>
</tr>
<tr>
<td>1.9.1.9 Viewing the Grid Node Tree</td>
<td>..........................................................</td>
<td>947</td>
</tr>
<tr>
<td>1.9.2 Chapter 38 DHCP Fingerprint Detection</td>
<td>..........................................................</td>
<td>947</td>
</tr>
<tr>
<td>1.9.2.1 Configuring DHCP Fingerprints</td>
<td>..........................................................</td>
<td>949</td>
</tr>
<tr>
<td>1.9.2.2 Enabling and Disabling DHCP Fingerprint Detection</td>
<td>..........................................................</td>
<td>950</td>
</tr>
<tr>
<td>1.9.2.3 Standard and Custom DHCP Fingerprints</td>
<td>..........................................................</td>
<td>951</td>
</tr>
<tr>
<td>1.9.3 Chapter 39 Monitoring with SNMP</td>
<td>..........................................................</td>
<td>951</td>
</tr>
<tr>
<td>1.9.3.1 Understanding SNMP</td>
<td>..........................................................</td>
<td>951</td>
</tr>
<tr>
<td>1.9.3.2 Configuring SNMP</td>
<td>..........................................................</td>
<td>953</td>
</tr>
<tr>
<td>1.9.3.3 SNMP MIB Hierarchy</td>
<td>..........................................................</td>
<td>978</td>
</tr>
<tr>
<td>1.9.4 Chapter 40 Infoblox Reporting and Analytics</td>
<td>..........................................................</td>
<td>1032</td>
</tr>
<tr>
<td>1.9.4.1 Setting Up Reporting and Analytics</td>
<td>..........................................................</td>
<td>1036</td>
</tr>
<tr>
<td>1.9.4.2 Supported Reporting Appliances and Storage Space</td>
<td>..........................................................</td>
<td>1036</td>
</tr>
<tr>
<td>1.9.4.3 Licensing Requirements</td>
<td>..........................................................</td>
<td>1037</td>
</tr>
<tr>
<td>1.9.4.4 Administrative Permissions</td>
<td>..........................................................</td>
<td>1038</td>
</tr>
<tr>
<td>1.9.4.5 Configuring an External Server for Search Result Exports</td>
<td>..........................................................</td>
<td>1039</td>
</tr>
<tr>
<td>1.9.4.6 About Reporting Clustering</td>
<td>..........................................................</td>
<td>1040</td>
</tr>
<tr>
<td>1.9.4.7 Guidelines for Deploying Reporting Clusters</td>
<td>..........................................................</td>
<td>1048</td>
</tr>
<tr>
<td>1.9.4.8 Grid Reporting Properties</td>
<td>..........................................................</td>
<td>1051</td>
</tr>
<tr>
<td>1.9.4.9 About IP Blocks and IP Block Groups</td>
<td>..........................................................</td>
<td>1055</td>
</tr>
<tr>
<td>1.9.4.10 Reporting User Interface Overview</td>
<td>..........................................................</td>
<td>1057</td>
</tr>
<tr>
<td>1.9.4.11 Home Dashboards</td>
<td>..........................................................</td>
<td>1059</td>
</tr>
<tr>
<td>1.9.4.12 About Alerts</td>
<td>..........................................................</td>
<td>1062</td>
</tr>
<tr>
<td>1.9.4.13 About Reports</td>
<td>..........................................................</td>
<td>1063</td>
</tr>
<tr>
<td>1.9.4.14 About Dashboards</td>
<td>..........................................................</td>
<td>1068</td>
</tr>
<tr>
<td>1.9.4.15 Managing Reporting Data</td>
<td>..........................................................</td>
<td>1098</td>
</tr>
<tr>
<td>1.9.5 Chapter 41 Reporting Data Model</td>
<td>..........................................................</td>
<td>1101</td>
</tr>
<tr>
<td>1.10 Part 8 Infoblox Infrastructure Security</td>
<td>..........................................................</td>
<td>1145</td>
</tr>
<tr>
<td>1.10.1 Chapter 42 Infoblox Advanced DNS Protection</td>
<td>..........................................................</td>
<td>1148</td>
</tr>
<tr>
<td>1.10.1.1 Configuring Infoblox Advanced DNS Protection</td>
<td>..........................................................</td>
<td>1150</td>
</tr>
<tr>
<td>1.10.1.2 Supporting Threat Protection Appliances and Licensing Requirements</td>
<td>..........................................................</td>
<td>1150</td>
</tr>
<tr>
<td>1.10.1.3 Administrative Permissions</td>
<td>..........................................................</td>
<td>1152</td>
</tr>
<tr>
<td>1.10.1.4 Starting and Stopping Threat Protection Service</td>
<td>..........................................................</td>
<td>1152</td>
</tr>
<tr>
<td>1.10.1.5 Enabling and Disabling Monitoring Mode</td>
<td>..........................................................</td>
<td>1152</td>
</tr>
<tr>
<td>1.10.1.6 Understanding Threat Protection Rulesets and Rules</td>
<td>..........................................................</td>
<td>1152</td>
</tr>
<tr>
<td>1.10.1.6.1 Packet Flow for Threat Protection Rules</td>
<td>..........................................................</td>
<td>1153</td>
</tr>
<tr>
<td>1.10.1.6.2 About Ruleset Versions and Updates</td>
<td>..........................................................</td>
<td>1154</td>
</tr>
<tr>
<td>1.10.1.6.3 System and Auto Rules</td>
<td>..........................................................</td>
<td>1155</td>
</tr>
<tr>
<td>1.10.1.6.4 Custom Rules</td>
<td>..........................................................</td>
<td>1156</td>
</tr>
<tr>
<td>1.10.1.6.5 Using the Events Per Second Rule Setting</td>
<td>..........................................................</td>
<td>1159</td>
</tr>
<tr>
<td>1.10.1.7 Configuring Grid Security Properties</td>
<td>..........................................................</td>
<td>1159</td>
</tr>
<tr>
<td>1.10.1.7.1 Enabling Multiple DNS Requests through a Single TCP Session</td>
<td>..........................................................</td>
<td>1160</td>
</tr>
<tr>
<td>1.10.1.8 Configuring NAT Mapping Properties</td>
<td>..........................................................</td>
<td>1160</td>
</tr>
<tr>
<td>1.10.1.8.1 Configuring NAT Mapping Rules</td>
<td>..........................................................</td>
<td>1161</td>
</tr>
<tr>
<td>1.10.1.9 Managing Threat Protection Rulesets</td>
<td>..........................................................</td>
<td>1161</td>
</tr>
<tr>
<td>1.10.1.9.1 Listing Members</td>
<td>..........................................................</td>
<td>1162</td>
</tr>
<tr>
<td>1.10.1.9.2 Viewing Threat Protection Rule Sets</td>
<td>..........................................................</td>
<td>1162</td>
</tr>
<tr>
<td>1.10.1.9.3 Activating a Rule Set</td>
<td>..........................................................</td>
<td>1162</td>
</tr>
<tr>
<td>1.10.1.9.4 Overriding the Grid Rule Set</td>
<td>..........................................................</td>
<td>1163</td>
</tr>
<tr>
<td>1.10.1.9.5 Modifying Rule Sets</td>
<td>..........................................................</td>
<td>1163</td>
</tr>
<tr>
<td>1.10.1.9.6 Comparing and Merging Rule Sets</td>
<td>..........................................................</td>
<td>1164</td>
</tr>
<tr>
<td>1.10.1.9.7 Manually Uploading Rule Sets</td>
<td>..........................................................</td>
<td>1164</td>
</tr>
<tr>
<td>1.10.1.9.8 Publishing Rule Updates</td>
<td>..........................................................</td>
<td>1165</td>
</tr>
<tr>
<td>1.10.1.10 Delegating Rule Updates to Grid Members</td>
<td>..........................................................</td>
<td>1165</td>
</tr>
<tr>
<td>1.10.1.11 Configuring Threat Protection Profiles</td>
<td>..........................................................</td>
<td>1165</td>
</tr>
<tr>
<td>1.10.1.11.1 Adding Threat Protection Profiles</td>
<td>..........................................................</td>
<td>1166</td>
</tr>
<tr>
<td>1.10.1.11.2 Cloning Threat Protection Profiles</td>
<td>..........................................................</td>
<td>1166</td>
</tr>
<tr>
<td>1.10.1.11.3 Modifying Threat Protection Profiles</td>
<td>..........................................................</td>
<td>1167</td>
</tr>
<tr>
<td>1.10.1.11.4 Merging Threat Protection Profiles</td>
<td>..........................................................</td>
<td>1167</td>
</tr>
<tr>
<td>1.10.1.11.5 Inheriting Grid Rule Settings</td>
<td>..........................................................</td>
<td>1168</td>
</tr>
<tr>
<td>1.10.1.11.6 Deleting Threat Protection Profiles</td>
<td>..........................................................</td>
<td>1168</td>
</tr>
<tr>
<td>1.10.1.11.7 Viewing Threat Protection Profiles</td>
<td>..........................................................</td>
<td>1168</td>
</tr>
<tr>
<td>1.10.1.12 Managing Threat Protection Rules</td>
<td>..........................................................</td>
<td>1169</td>
</tr>
</tbody>
</table>
1.10.1.12.1 Viewing Threat Protection Rules .......................................................... 1169
1.10.1.12.2 Enabling and Disabling Rules ............................................................... 1170
1.10.1.12.3 Modifying System and Auto Rules ....................................................... 1171
1.10.1.12.4 Modifying Custom Rules ........................................................................ 1171
1.10.1.13 Monitoring Threat Protection Events ....................................................... 1171
  1.10.1.13.1 Monitoring through Syslog ................................................................. 1172
  1.10.1.13.2 Threat Protection Statistics Widget .................................................... 1172
  1.10.1.13.3 Threat Protection Reports .................................................................... 1172
1.10.1.14 DNS and Network-Flood Threats .............................................................. 1173
  1.10.1.14.1 Internet Control Message Protocol (ICMP) Flood ............................... 1173
  1.10.1.14.2 SYN Flood ......................................................................................... 1173
  1.10.1.14.3 UDP DNS Flood ................................................................................ 1173
  1.10.1.14.4 Inside-Out Attacks ............................................................................. 1173
  1.10.1.14.5 DNS Fluxing ....................................................................................... 1173
  1.10.1.14.6 DNS Cache Poisoning ........................................................................ 1173
  1.10.1.14.7 DNS Reflection and Amplification Attacks ........................................... 1173
  1.10.1.14.8 DNS Malware ..................................................................................... 1174
  1.10.1.14.9 DNS Domain Hijacking ....................................................................... 1174
1.10.2 Chapter 43 Infoblox DNS Firewall ................................................................. 1174
  1.10.2.1 License Requirements and Admin Permissions for RPZ ............................ 1177
  1.10.2.2 Best Practices for Configuring RPZs ......................................................... 1179
  1.10.2.3 Enabling Recursion for RPZs ................................................................... 1180
  1.10.2.4 Configuring Local RPZs ........................................................................... 1181
  1.10.2.5 Configuring Rules for RPZs .................................................................... 1182
  1.10.2.6 Configuring Infoblox Threat Intelligence Feed ........................................ 1191
  1.10.2.7 Downloading Rules for an RPZ Feed ....................................................... 1193
  1.10.2.8 Testing RPZ Feed Rules .......................................................................... 1193
  1.10.2.9 About FireEye Integrated RPZs ................................................................. 1194
  1.10.2.10 Mitigating Cyber Threats using TAXII ................................................... 1199
  1.10.2.11 Managing RPZs ...................................................................................... 1201
  1.10.2.12 Managing RPZ Rules ............................................................................. 1203
  1.10.2.13 Configuring Prefix Length Limit for RPZ-IP Triggers ......................... 1205
  1.10.2.14 Configuring Thresholds for RPZ Hit Rate ............................................. 1206
  1.10.2.15 Verifying RPZ Configuration ................................................................. 1207
1.10.3 Chapter 44 Cisco ISE Integration ................................................................. 1208
  1.10.3.1 Integrating Cisco ISE into NIOS .............................................................. 1209
  1.10.3.2 Configuring Cisco ISE on NIOS .............................................................. 1210
  1.10.3.3 Publishing Data ....................................................................................... 1212
1.10.4 Chapter 45 Ecosystem - Outbound Notifications .......................................... 1215
  1.10.4.1 Outbound Notification Overview ............................................................ 1215
  1.10.4.2 Configuring Outbound Notifications ..................................................... 1217
  1.10.4.3 About Outbound Templates .................................................................... 1217
  1.10.4.4 Configuring Outbound Endpoints ........................................................... 1268
  1.10.4.5 Configuring Notification Rules ............................................................... 1271
  1.10.4.6 Sample Templates .................................................................................. 1273
1.10.5 Chapter 46 Infoblox Threat Insight .............................................................. 1284
  1.10.5.1 About Infoblox Threat Insight ............................................................... 1296
1.11 Part 9 Reference ............................................................................................... 1302
  1.11.1 Appendix A Glossary of Terms ................................................................... 1303
  1.11.2 Appendix B Grid Manager Icons .................................................................. 1309
  1.11.3 Appendix C Guidance Documentation Supplement for Common Criteria .... 1314
    1.11.3.1 Pre-Requisites ..................................................................................... 1314
    1.11.3.2 Verifying the Hardware ...................................................................... 1315
    1.11.3.3 Security Guidelines .......................................................................... 1315
    1.11.3.4 Administration .................................................................................... 1316
    1.11.3.5 Enabling / Disabling Common Criteria Mode ....................................... 1316
    1.11.3.6 Licenses and Services ....................................................................... 1317
    1.11.3.7 WebUI Settings .................................................................................. 1317
    1.11.3.8 Backing Up and Restoring the Database .......................................... 1318
    1.11.3.9 Secure Syslog Transport ................................................................... 1318
    1.11.3.10 Audit Log ......................................................................................... 1319
    1.11.3.11 Syslog ....................................................................................... 1322
  1.11.4 Appendix D Guidance Documentation Supplement for Federal Information Processing Standard .................................................................................. 1325
    1.11.4.1 Managing Administrators ................................................................... 1326
    1.11.4.2 Authenticating Admins using Remote Authentication ......................... 1327
    1.11.4.3 Enabling/Disabling FIPS .................................................................. 1328
    1.11.4.4 Installing FIPS Label on an Infoblox Trinzic Appliance ...................... 1328
    1.11.4.5 FIPS (Federal Information Processing Standard) Certification ........... 1329
    1.11.4.6 List of NIOS Algorithms .................................................................. 1392
  1.11.5 Appendix E Regular Expressions ................................................................... 1433
    1.11.5.1 Supported Expressions for Search Parameters ................................. 1433
  1.11.6 Appendix F NIOS Virtual Appliances ......................................................... 1434
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.11.6.1 NIOS for VMware</td>
<td>1436</td>
</tr>
<tr>
<td>1.11.6.2 NIOS for Hyper-V</td>
<td>1436</td>
</tr>
<tr>
<td>1.11.6.3 NIOS for Xen</td>
<td>1436</td>
</tr>
<tr>
<td>1.11.7 Appendix G Product Compliance</td>
<td>1437</td>
</tr>
<tr>
<td>1.11.7.1 AC</td>
<td>1437</td>
</tr>
<tr>
<td>1.11.7.2 DC</td>
<td>1437</td>
</tr>
<tr>
<td>1.11.7.3 Agency Compliance</td>
<td>1438</td>
</tr>
<tr>
<td>1.11.7.4 RFC Compliance</td>
<td>1438</td>
</tr>
<tr>
<td>1.11.8 Appendix H Open Source Copyright and License Statements</td>
<td>1442</td>
</tr>
<tr>
<td>1.11.8.1 GNU Lesser General Public License</td>
<td>1445</td>
</tr>
<tr>
<td>1.11.8.2 Apache Software License, Version 2.0</td>
<td>1448</td>
</tr>
<tr>
<td>1.11.8.3 perl Artistic License</td>
<td>1450</td>
</tr>
<tr>
<td>1.11.8.4 ISC BIND Copyright</td>
<td>1451</td>
</tr>
<tr>
<td>1.11.8.5 ISC DHCP Copyright</td>
<td>1451</td>
</tr>
<tr>
<td>1.11.8.6 Julian Seward Copyright</td>
<td>1451</td>
</tr>
<tr>
<td>1.11.8.7 Carnegie Mellon University Copyright</td>
<td>1452</td>
</tr>
<tr>
<td>1.11.8.8 Thai Open Source Software Center Copyright</td>
<td>1452</td>
</tr>
<tr>
<td>1.11.8.9 Ian F. Darwin Copyright</td>
<td>1452</td>
</tr>
<tr>
<td>1.11.8.10 Lawrence Berkeley Copyright</td>
<td>1453</td>
</tr>
<tr>
<td>1.11.8.11 MIT Kerberos Copyright</td>
<td>1453</td>
</tr>
<tr>
<td>1.11.8.12 BSD License</td>
<td>1453</td>
</tr>
<tr>
<td>1.11.8.13 David L. Mills Copyright</td>
<td>1454</td>
</tr>
<tr>
<td>1.11.8.14 OpenLDAP License</td>
<td>1454</td>
</tr>
<tr>
<td>1.11.8.15 OpenSSL License</td>
<td>1454</td>
</tr>
<tr>
<td>1.11.8.16 VIM License</td>
<td>1455</td>
</tr>
<tr>
<td>1.11.8.17 ZLIB License</td>
<td>1456</td>
</tr>
<tr>
<td>1.11.8.18 Wietse Venema Copyright</td>
<td>1456</td>
</tr>
<tr>
<td>1.11.8.19 ECLIPSE SOFTWARE</td>
<td>1456</td>
</tr>
<tr>
<td>1.11.8.20 Eclipse Public License - v 1.0</td>
<td>1456</td>
</tr>
<tr>
<td>1.11.8.21 AOP Alliance (Java/J2EE AOP standards)</td>
<td>1458</td>
</tr>
<tr>
<td>1.11.8.22 OpenJDK</td>
<td>1458</td>
</tr>
<tr>
<td>1.11.8.23 TASM</td>
<td>1461</td>
</tr>
<tr>
<td>1.11.8.24 Distributed Computing Laboratory, Emory University</td>
<td>1462</td>
</tr>
<tr>
<td>1.11.8.25 COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL)</td>
<td>1462</td>
</tr>
<tr>
<td>1.11.8.26 The FreeType Project LICENSE</td>
<td>1465</td>
</tr>
<tr>
<td>1.11.8.27 The Independent JPEG Group's JPEG software</td>
<td>1466</td>
</tr>
<tr>
<td>1.11.8.28 Net-SNMP</td>
<td>1467</td>
</tr>
<tr>
<td>1.11.8.29 The PHP License, version 3.01</td>
<td>1470</td>
</tr>
<tr>
<td>1.11.8.30 INFO-ZIP</td>
<td>1470</td>
</tr>
<tr>
<td>1.11.8.31 MIT License</td>
<td>1471</td>
</tr>
<tr>
<td>1.11.8.32 Ehcache</td>
<td>1471</td>
</tr>
<tr>
<td>1.11.8.33 Cybox</td>
<td>1471</td>
</tr>
<tr>
<td>1.11.8.34 Dateutil</td>
<td>1472</td>
</tr>
<tr>
<td>1.11.8.35 Importlib</td>
<td>1472</td>
</tr>
<tr>
<td>1.11.8.36 Libtaxii</td>
<td>1472</td>
</tr>
<tr>
<td>1.11.8.37 Mixbox</td>
<td>1473</td>
</tr>
<tr>
<td>1.11.8.38 Stix</td>
<td>1473</td>
</tr>
<tr>
<td>1.11.8.39 PSF License Agreement for Python 2.6</td>
<td>1473</td>
</tr>
<tr>
<td>1.11.8.40 PSF License Agreement for Python 3.5.0</td>
<td>1474</td>
</tr>
<tr>
<td>1.11.8.41 GNU General Public License 2.0 for Suricata, Netfilter and IPTables</td>
<td>1474</td>
</tr>
<tr>
<td>1.11.8.42 LibYAML</td>
<td>1477</td>
</tr>
<tr>
<td>1.11.8.43 The MIT License for Jansson</td>
<td>1477</td>
</tr>
<tr>
<td>1.11.8.44 PCRE - Perl Compatible Regular Expressions</td>
<td>1477</td>
</tr>
<tr>
<td>1.11.9 Appendix I Configuration Requiring Service Restart</td>
<td>1478</td>
</tr>
</tbody>
</table>
Preface

This preface describes the document conventions of this guide, and provides information about how to find additional product information, including accessing Infoblox Technical Support. It includes the following sections:

- Related Documentation
- Customer Care
  - User Accounts
  - Software Upgrades
  - Technical Support

Related Documentation

Other Infoblox documentation:
- Infoblox CLI Guide
- Infoblox API Documentation
- Infoblox WAPI Documentation
- Infoblox CSV Import Reference
- Infoblox Installation Guide for the Trinzic 100 Appliance
- Infoblox Installation Guide for the 800 Series Platforms
- Infoblox Installation Guide for the 805 Series Platforms
- Infoblox Installation Guide for the 1400 Series Platforms
- Infoblox Installation Guide for the 1405 Series Platforms
- Infoblox Installation Guide for the 2200 Series Platforms
- Infoblox Installation Guide for the 2205 Series Platforms
- Infoblox Installation Guide for the 4000 Series Platforms
- Infoblox Installation Guide for the Infoblox-4010 Appliance
- Infoblox Installation Guide for the IB-4030 and IB-4030-10GE Appliances
- Infoblox DNS Cache Acceleration Administrator Guide
- Infoblox Installation Guide for vNIOS for Microsoft Azure
- Infoblox Installation Guide for vNIOS for AWS
- Infoblox Installation Guide for vNIOS for VMware
- Infoblox Installation Guide for vNIOS on Microsoft 2008 R2 for Hyper-V
- Infoblox Installation Guide for vNIOS for KVM Hypervisor and KVM-based OpenStack
- Infoblox Safety Guide

To provide feedback on any of the Infoblox technical documents, please e-mail techpubs@infoblox.com.

Customer Care

This section addresses user accounts, software upgrades, licenses and warranties, and technical support.

User Accounts

The Infoblox appliance ships with a default user name and password. Change the default admin account password immediately after the system is installed to safeguard its use. Make sure that the NIOS appliance has at least one administrator account with superuser privileges at all times, and keep a record of your account information in a safe place. If you lose the admin account password, and did not already create another superuser account, the system will need to be reset to factory defaults, causing you to lose all existing data on the NIOS appliance. You can create new administrator accounts, with or without superuser privileges. For more information, see Managing Administrators.

Software Upgrades

Software upgrades are available according to the Terms of Sale for your system. Infoblox notifies you when an upgrade is available. Register immediately with Infoblox Technical Support at http://www.infoblox.com/support/customer/evaluation-and-registration to maximize your Technical Support.

Technical Support

Infoblox Technical Support provides assistance via the Web, e-mail, and telephone. The Infoblox Support web site at https://support.infoblox.com provides access to product documentation and release notes, but requires the user ID and password you receive when you register your product online at: http://www.infoblox.com/support/customer/evaluation-and-registration.

Documentation Conventions
The text in this guide follows the following style conventions.

<table>
<thead>
<tr>
<th>Style</th>
<th>Usage</th>
</tr>
</thead>
</table>
| bold      | • Indicates anything that you input in the user interface, by clicking, choosing, selecting, typing, or by pressing on the keyboard.  
|           | • Indicates the field names in the user interface.                   |
| input     | Signifies command line entries that you type.                        |
| variable  | Signifies variables typed into the user interface that you need to modify specifically for your configuration. These can be command line variables, file names, and keyboard characters. |
|           | Indicates the names of the wizards, editors, and dialog boxes in Grid Manager, such as the Add Network wizard or the DHCP Network editor. |

Variables

Infoblox uses the following variables to represent values that you type, such as file names and IP addresses.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>a_record</td>
<td>A record</td>
</tr>
<tr>
<td>aaaa_record</td>
<td>AAAA record</td>
</tr>
<tr>
<td>admin_group</td>
<td>Name of a group of administrators</td>
</tr>
<tr>
<td>admin_name</td>
<td>Name of the appliance administrator</td>
</tr>
<tr>
<td>addr_range</td>
<td>IP address range</td>
</tr>
<tr>
<td>dhcp_template</td>
<td>DHCP template</td>
</tr>
<tr>
<td>domain_name</td>
<td>Domain name</td>
</tr>
<tr>
<td>directory</td>
<td>Directory name</td>
</tr>
<tr>
<td>failover_association</td>
<td>Failover association</td>
</tr>
<tr>
<td>filter_name</td>
<td>Name of a DHCP filter</td>
</tr>
<tr>
<td>fingerprint</td>
<td>DHCP fingerprint</td>
</tr>
<tr>
<td>fixed_address</td>
<td>Fixed address</td>
</tr>
<tr>
<td>fixed_address_template</td>
<td>Fixed address template</td>
</tr>
<tr>
<td>glb</td>
<td>Global Load Balancer</td>
</tr>
<tr>
<td>Grid</td>
<td>Grid name</td>
</tr>
<tr>
<td>Grid_master</td>
<td>Grid Master</td>
</tr>
<tr>
<td>Grid_member</td>
<td>Grid Member</td>
</tr>
<tr>
<td>hostname</td>
<td>Host name of an independent appliance</td>
</tr>
<tr>
<td>host_record</td>
<td>Host record</td>
</tr>
<tr>
<td>ifmap_client</td>
<td>IF-MAP client</td>
</tr>
<tr>
<td>ip_addr</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>lease</td>
<td>IP address of a lease</td>
</tr>
<tr>
<td>mac_filter</td>
<td>Name of a MAC filter</td>
</tr>
<tr>
<td>match_rule</td>
<td>Name of a match rule</td>
</tr>
<tr>
<td>member</td>
<td>Grid member name</td>
</tr>
</tbody>
</table>
Part 1 Appliance GUI

This section introduces you to Grid Manager, the web interface through which you can manage your DNS, DHCP and IP address management (IPAM) infrastructure. It also describes the Task and Status Dashboards, your home page on Grid Manager, and Smart Folders, which you can use to organize your data.

It includes the following chapters:

- Chapter 1, Infoblox Grid Manager
- Chapter 2, Dashboards
- Chapter 3, Smart Folders

Chapter 1 Infoblox Grid Manager

This chapter lists requirements for the management system you use to access the NIOS appliance. It also explains how to access the Grid Manager web interface and describes its major components. This chapter includes the following sections:

- bookmark13
- bookmark16
- Browser Limitations
- About Grid Manager
  - Admin Permissions for Grid Manager
  - Logging in to the GUI
• Setting Login Options
  • Specifying the Grid Name and Hostname
  • Creating a Login Banner
  • Changing the Password and Email Address
  • Specifying the Table Size
  • Selecting Your Home Page
  • Setting the Browser Time Zone
• Opening Technical Support Requests
• SSL and TLS Protocols
• Managing Certificates
  • About HTTPS Certificates
  • About Client Certificates
• About the Grid Manager Interface
  • System Messages
  • Security and Informational Banners
  • Breadcrumbs Navigation
  • Global Search
  • Finder Panel
  • Toolbar Panel
  • Help Panel
  • Wizards and Editors
  • Tooltips
  • Customizing Tables
  • Selecting Objects in Tables
• Modifying Data in Tables
• Finding and Restoring Data
  • Using Bookmarks
  • Using the Recycle Bin
  • Managing Third Party URL Links
  • Using Filters
  • Using Quick Filters
  • Using Global Search
  • Using the Go To Function
• About Tasks
  • Viewing Tasks
  • Supported Objects for Scheduled and Approval Tasks
  • Guidelines for Upgrading, Backing Up, and Restoring Data
• Scheduling New IPAM/DHCP Objects and Associated Port Configurations
• Scheduling Creation of new IPv4/IPv6 Networks and Associated Device Provisioning
• Scheduling Tasks
  • Scheduling Additions and Modifications
  • Scheduling Appliance Operations
  • Scheduling Deletions
  • Scheduling Recursive Deletions of Network Containers and Zones
  • Viewing Scheduled Tasks
  • Rescheduling Tasks
  • Canceling Scheduled Tasks
• Configuring Approval Workflows
  • Creating Approval Workflows
  • Viewing Approval Workflows
  • Modifying Approval Workflows
  • Deleting Approval Workflows
  • Viewing Approval Tasks
  • Viewing Workflow Notifications
  • Unsupported Operations for Submitters
• About Long Running Tasks
  • Running Tasks in the Background
  • Monitoring Long Running Tasks
• About CSV Import
  • CSV Import User Permissions
  • CSV Import Limitations
  • Configuring Import Options
  • Viewing CSV Import Jobs
  • Modifying CSV Import Jobs
  • Deleting Uploaded Jobs
  • Downloading Files
  • Creating a Data File for Import
  • Exporting Data to Files
• Exporting Displayed Data
• Printing from Grid Manager
Management System Requirements
The management system is the computer from which you configure and manage the NIOS appliance. The management system must meet the following requirements.

Figure 1.1 Software and Hardware Requirements for the Management System

<table>
<thead>
<tr>
<th>Management System Software Requirements</th>
<th>Management System Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI ACCESS</td>
<td>• Minimum System:</td>
</tr>
<tr>
<td>• See bookmark16 for details.</td>
<td>1.4 GHz CPU with 1 GB RAM available to the product GUI, and 256 Kbps connectivity to NIOS appliance</td>
</tr>
<tr>
<td>CLI ACCESS</td>
<td>• Recommended System:</td>
</tr>
<tr>
<td>• Secure Socket Shell (SSH) client that supports SSHv2</td>
<td>2.0 GHz (or higher) dual core CPU with 2 GB RAM available for the product GUI, and network connectivity to NIOS appliance</td>
</tr>
<tr>
<td>• Terminal emulation program, such as minicom or Hilgraeve Hyperterminal®</td>
<td>• Monitor Resolution: 1280 x 768 (minimum) 1280 x 1024 or better (recommended)</td>
</tr>
</tbody>
</table>

Supported Browsers
Grid Manager supports the following operating systems and browsers. You must install and enable Javascript for Grid Manager to function properly. Grid Manager supports only SSL version 3 and TLS version 1 connection.

Infoblox recommends that you use a computer that has a 2 GHz CPU and at least 1 GB of RAM. Infoblox supports the following browsers for Grid Manager:

<table>
<thead>
<tr>
<th>OS</th>
<th>Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 8.0 and 8.1®</td>
<td>Microsoft Internet Explorer® 11.x*, 10.x* Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x</td>
</tr>
<tr>
<td>Microsoft Windows 7®</td>
<td>Microsoft Internet Explorer® 11.x*, 10.x*, 9.x, and 8.x Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x</td>
</tr>
<tr>
<td>Microsoft Windows XP® (SP2+)</td>
<td>Microsoft Internet Explorer 7.x and 8.x Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x</td>
</tr>
<tr>
<td>Red Hat® Enterprise Linux® 7.x</td>
<td>Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x</td>
</tr>
<tr>
<td>Red Hat® Enterprise Linux® 6.x</td>
<td>Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x</td>
</tr>
<tr>
<td>Red Hat® Enterprise Linux® 5.x</td>
<td>Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x</td>
</tr>
<tr>
<td>Apple® Mac OS X 10.11.x</td>
<td>Safari 9.x, 8.x, 7.x Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x</td>
</tr>
<tr>
<td>Apple® Mac OS X 10.10.x</td>
<td>Safari 8.x, 7.x Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x</td>
</tr>
<tr>
<td>Apple® Mac OS X 10.9.x</td>
<td>Safari 7.x Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x</td>
</tr>
<tr>
<td>Apple® Mac OS X 10.8.x</td>
<td>Safari 6.x Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x</td>
</tr>
<tr>
<td>Apple® Mac OS X 10.7.x</td>
<td>Safari 5.x Mozilla Firefox 32.x, 31.x, 25.x, 21.x, 16.x, and 10.x Google Chrome 37.x, 36.x, 30.x, 27.x, 22.x, and 16.x</td>
</tr>
</tbody>
</table>
Before you log in to Grid Manager, ensure that you have installed your NIOS appliance as described in the installation guide or user guide that shipped with your product. You can then access Grid Manager using one of the supported browsers. For information, see **Supported Browsers**.

### Admin Permissions for Grid Manager

You can log in to Grid Manager as long as you have permission to log in to the NIOS appliance. Superusers have unrestricted access to Grid Manager. Limited-access users though, require read-only or read-write permission to the data that they want to manage through Grid Manager. Grid Manager allows limited-access users to view and manage only the data for which they have permission. For example, to view IPv4 networks, you must have at least read-only permission to IPv4 networks. To run a discovery, you must have read/write permission to the Network Discovery feature.

Note that superusers must configure admin groups and accounts in the Grid Manager application of the NIOS appliance. In Grid Manager, superusers can set and change permissions for specific objects, such as IPv4 networks, IPv6 networks, and resource records. For information about user accounts and administrative permissions, see **Managing Administrators**.

### Logging in to the GUI

Before you log in to Grid Manager, ensure that you have installed your NIOS appliance as described in the installation guide or user guide that shipped with your products and configured it accordingly. You must upload the CA certificate(s) that issued the client certificate to ensure a successful SSL/TLS connection to the appliance.

To log in to Grid Manager:

1. Open an Internet browser window and enter **https://<IP address or hostname of your NIOS appliance>**. The Grid Manager login page

---

**Note:** Grid Manager fully supports Microsoft Internet Explorer® 11.x and 10.x when you enable compatibility view in the browser. Features in the **Reporting** tab may not function properly if you disable compatibility view. In the browser, go to **Tools -> Compatibility View** to enable the feature.

Infoblox recommends using the latest release of the supported versions of Internet Explorer, Mozilla Firefox or Google Chrome for best performance.

### Browser Limitations

- When you use Internet Explorer 7 or 8 without installing the latest updates, Grid Manager may stop loading a page when you navigate from one tab to another or when you use the back navigation button to go back to a previous page. To solve this problem, you can press Ctrl+F5 to refresh the browser or install the latest updates.
- When you use the zoom function in Internet Explorer 7 running on Microsoft Windows XP, Grid Manager may not properly display some pop up windows. This is a known issue in Internet Explorer 7.
- In Internet Explorer 8, Grid Manager does not display the directory path of an uploaded file. Instead, it displays "failepath" in place of the directory path. To resolve this issue, you can add Grid Manager as a trusted site or enable the "Include local directory path when uploading files to a server" feature in the browser. For information, refer to the MSDN documentation at https://msdn.microsoft.com/en-us/library/ms535128.aspx.
- When you use Firefox to access Grid Manager, tooltips do not display for disabled drop-down menu items. In addition, when you run a large query of smart folders, Grid Manager may display a warning message about "Unresponsive Script". Click **Continue** to proceed.
- Depending on the browser you use, Grid Manager may display a dialog box that indicates the system is unavailable during a system restart or reboot.
- Infoblox strongly recommends that you do not log in to Grid Manager from different browser windows using the same user account. Depending on the browser you use, it may cache user information in one session and apply it to another session. This can cause inconsistent behaviors within the browser sessions.

### About Grid Manager

Grid Manager is the web interface that provides access to your appliance for network and IP address management. It provides a number of tools that you can use to effectively manage your appliance and IP address space.

- Use Smart Folders to organize your data based on criteria you specify. For information, see **Smart Folders**.
- The network and IP address maps and lists provide views of your networks and IP addresses, so you can quickly evaluate IP address usage and understand how your network resources are being utilized. You can quickly determine which IP addresses are in use, when they were allocated, and to which devices they were assigned. For information, see **Chapter 13, IP Address Management**.
- Customize the Dashboard to monitor your Grid and networks. The Dashboard also provides access to frequently-used commands and the network discovery feature. You can run network discoveries to identify IP address conflicts and troubleshoot network issues. For information, see **Dashboards**.
- Tools such as the **Finder** panel, filters, and global search help you quickly find the information you need. For information, see **About the Grid Manager Interface**.
- Use wizards to quickly create new networks and resource records. Editors allow you to configure additional operational parameters. For information, see **Wizards and Editors**.

Before you can use Grid Manager, you must install and configure the NIOS appliance as described in the installation guide that shipped with your product. You can then access Grid Manager using one of the supported browsers. For information, see **Supported Browsers**.
Setting Login Options
Grid Manager provides several options that you can set to facilitate the login process. Additionally, you can manage CA (Certificate Authority) and server certificates on the NIOS appliance. You can import certificates, select and view their details, or remove them. To manage certificates, see Managing Certificates.

Specifying the Grid Name and Hostname
To define the default hostname that appears when the login prompt displays:

1. From the Grid tab, select the Grid Manager tab, and then click Grid Properties -> Set up (Grid Setup Wizard) from the Toolbar.
2. On the Welcome page, select Configure a Grid Master, and then click Next.
3. Enter the Grid name in the Grid Name field and the hostname in the Host Name field.

Creating a Login Banner
You can create a statement that appears at the top of the Login screen (a banner message). This function is useful for posting security warnings or user-friendly information well above the user name and password fields on the Login screen. A login banner message can be up to 3000 characters long. In a Grid, perform this task on the Grid Master.
To create a login banner:

1. From the Grid tab, select the Grid Manager tab, and then click Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the Security tab, and then select Enable Login Banner. In the text field, enter the text that you want displayed on the login screen.
3. Save the configuration.

Changing the Password and Email Address
Grid Manager creates and stores a user profile for each admin user. Each user profile contains information about the admin group and admin type assigned to the user. You can modify certain information in your user profile any time after the initial login. You can change your password to facilitate future logins and add your email address for reference.
Note that when multiple users log in to Grid Manager using the same admin account, they share the same user profile and preference settings, such as the widget, table size and column settings, independent of their browser settings. Instead of using the same admin account for multiple users, you can add multiple users to the same admin group so they can share the same permissions. For more information about configuring admin accounts and admin groups, see Managing Administrators.

If you can access only the Tasks Dashboard, you may not see or configure certain fields in the User Profile editor.
To change your password and email address:

1. At the top right corner of the navigation bar, click the Admin name and select Profile from the drop-down menu.
2. In the User Profile editor, complete the following:
   - Name: Displays your user name.
   - Last Login: Displays the timestamp of your last login.
   - Type: Displays your user type. There are two user types: Local and Remote. The local admin accounts are stored in the
database of the appliance, and the remote admin accounts are stored on another server, such as a RADIUS server. Grid Manager automatically deletes remote user profiles if the users have not logged in for more than six months.

- **Group**: Displays the admin group to which your account belongs. The admin group determines your administrative permissions. Only superusers can define admin groups through Grid Manager.
- **Password**: You can set a new password according to the requirements that are displayed.
  - **Set Password**: If you are a local user, select this check box to set a new password for your account. If you are a remote user, this field does not appear.
  - **Old Password**: Enter your current password.
  - **New Password**: Enter the new password, and then re-enter it in the Retype Password field.
- **Email Address**: Enter your email address. Note that this address simply provides contact information. By default, this field is blank.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

### Specifying the Table Size

You can specify the amount of data Grid Manager can display in a table or a single list view. You can improve the display performance by setting a smaller table size. The setting you specify here applies to all tables in Grid Manager. Note that if you can access only the Tasks Dashboard, you cannot configure table size.

To specify table size:

1. At the top right corner of the navigation bar, click the Admin name and select **Profile** from the drop-down menu.
2. In the **User Profile** editor, complete the following:
   - **Table Size**: Specify the number of lines of data you want a table or a single list view to contain. You can set the number of lines from 10 to 256. The default is 20.
3. Save the configuration and click **Restart** if it appears at the top of the screen.

### Selecting Your Home Page

When you first log in to Grid Manager, the Tasks Dashboard is your home page. You can change your home page for subsequent logins. You can specify the maximum number of widgets that can be configured per dashboard. You can set up to 20 widgets per dashboard. You can also set the auto refresh rate for the dashboard widgets. This interval tells how often the content of the dashboard widgets are refreshed.

To change your home page:

1. At the top right corner of the navigation bar, click the Admin name and select **Profile** from the drop-down menu.
2. In the **User Profile** editor, complete the following:
   - **Default Dashboard**: Select **Status** or **Task** from the drop-down list.
   - **Maximum Widgets per Dashboard**: Specify the maximum number of widgets that can be configured per Dashboard. You can enter a value between 1 and 20. The default value is 10. This limit does not apply to the default dashboard.
   - **Auto-refresh rate**: Specify the time interval in seconds the appliance refreshes the content of the widget automatically. The default auto-refresh rate is 10 seconds.
3. Save the configuration and click **Restart** if it appears at the top of the screen.

Grid Manager displays the selected dashboard as your home page when you log in the next time.

### Setting the Browser Time Zone

You can specify the time zone Grid Manager uses to convert all displayed time values such as the last discovered and last login time. Grid Manager sets the time zone based on the time zone of your browser when you set the time zone to auto-detect in the **User Profile** editor. When you set the time zone of your browser to auto-detect and Grid Manager cannot automatically determine the time zone when you log in, the time zone is set to UTC (Coordinated Universal Time) standard. In this case, you can manually change the time zone in the **User Profile** editor. To manually set the time zone of your browser:

1. At the top right corner of the navigation bar, click the Admin name and select **Profile** from the drop-down menu. The **User Profile** editor displays your user name, user type, and admin group.
2. In the **User Profile** editor, complete the following:
   - **Time Zone**: Select the time zone Grid Manager uses to convert all displayed time values. The default is **Auto-detect time zone**. You must select a specific time zone when Grid Manager cannot automatically detect the time zone of your browser.
3. Save the configuration and click **Restart** if it appears at the top of the screen.

### Opening Technical Support Requests

When you encounter product issues or require assistance, you can send a request to Infoblox Technical Support by opening a support case through Grid Manager. When you submit a support case, product information such as software version and serial number is automatically collected from the NIOS appliance on which you create the support case. You should however provide detailed information about the issue or your request, business impact, and contact information to ensure that the support request is being addressed by the appropriate resources in a timely manner. When you submit a support request, Infoblox Technical Support automatically authenticates and authorizes the contact email address that you use. It sends a confirmation email to the contact email address if the email address is registered on the Infoblox Technical Support server. If the authentication fails, you will receive an email.
Complete the following to create a support case:

1. **Admin**: At the top right corner of the navigation bar, click the Admin name and select **Open a Support Case** from the drop-down menu.

   **Support**: From the Help panel -> click **Support** -> **Open a Support Case**.

   **Note**: Click **Go to the Editor** and enable **DNS Resolver** or **Use SMTP Relay** if you have not already enabled either one of them.

2. In the **Open Support Case** editor, complete the following:

   - **To Email Address**: Enter an email address to access Infoblox Technical support. The default is `support@infoblox.com`. If you change the default email address, the email is sent to the updated email address instead of Infoblox Technical Support. Sending the email to your own email address allows you to verify and alter the email content before you forward the email to `support@infoblox.com` or another email address.
   - **Contact Email Address**: Enter your email address or another contact email to which a confirmation is sent when the support case is created. Ensure that the contact email is legitimate and approved by Infoblox as this contact becomes the primary contact for the support case.
   - **CC Email Addresses**: Click the Add icon to add additional email addresses. This is optional.
   - **Case Type**: From the drop-down menu, select the case type:
     - **Administrative Issue**: Select this if the request is related to administrative issues.
     - **Administrative Question**: Select this if you have administrative questions.
     - **Product Issue**: Select this if the request is related to product issues.
     - **Product Question**: Select this if you have questions about Infoblox products.
   - **Severity**: Select how urgent or severe this request affects your business.
     - **Low**: Select this if the business impact is low.
     - **Medium**: Select this if the issue has moderate impact on your business.
     - **High**: Select this if this issue is urgent and requires immediate attention.
   - **Subject**: Enter a subject line for your support case.
   - **Description**: Enter a detailed description about the issue.
   - **Attach a file**: You can attach a file that contains additional information about your support case. Relevant information can help the Infoblox Support team to identify problems and troubleshoot issues in a more efficient manner.

3. Click **Send&Close** to create the support case. Optionally, click **Send&New** to send the current request and then create a new support request.

   **Note**: It might take up to 15 minutes before you get an email confirmation.

### SSL and TLS Protocols

When you log in to the NIOS appliance, your computer makes an HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer protocol) connection to the NIOS appliance. HTTPS is the secure version of HTTP, the client-server protocol used to send and receive communications throughout the Web. HTTPS uses SSL (Secure Sockets Layer) and/or TLS (Transport Layer Security) protocols to secure the connection between a client and server. SSL/TLS provides server authentication and encryption. The NIOS appliance supports TLS versions 1.0, 1.1, and 1.2. TLS provides cipher suites that are used to negotiate the security settings for the secure connection. Infoblox has provided a few CLI commands so you can enable and disable specific cipher suites. For detailed information about these CLI commands, refer to the **Infoblox CLI Guide**.

Note that enabling or disabling the TLS ciphers will enable or disable the equivalent SSHd cipher. The following table lists the TLS suite name and the corresponding OpenSSL suite name, SSHd cipher name, and SSHd MAC name:

<table>
<thead>
<tr>
<th>TLS Suite Name</th>
<th>Open SSL Suite Name</th>
<th>SSHd Cipher</th>
<th>SSHd MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA</td>
<td>DHE-RSA-AES256-SHA</td>
<td>aes256-cbc</td>
<td>hmac-sha1, <a href="mailto:hmac-sha1-etc@openssl.com">hmac-sha1-etc@openssl.com</a></td>
</tr>
<tr>
<td>TLS_DHE_DSS_WITH_AES_256_CBC_SHA</td>
<td>DHE-DSS-AES256-SHA</td>
<td>aes256-cbc</td>
<td>hmac-sha1, <a href="mailto:hmac-sha1-etc@openssl.com">hmac-sha1-etc@openssl.com</a></td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA</td>
<td>AES256-SHA</td>
<td>aes256-cbc</td>
<td>hmac-sha1, <a href="mailto:hmac-sha1-etc@openssl.com">hmac-sha1-etc@openssl.com</a></td>
</tr>
<tr>
<td>TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA</td>
<td>EDH-RSA-DES-CBC3-SHA</td>
<td>3des-cbc</td>
<td>hmac-sha1, <a href="mailto:hmac-sha1-etc@openssl.com">hmac-sha1-etc@openssl.com</a></td>
</tr>
<tr>
<td>TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA</td>
<td>EDH-DSS-DES-CBC3-SHA</td>
<td>3des-cbc</td>
<td>hmac-sha1, <a href="mailto:hmac-sha1-etc@openssl.com">hmac-sha1-etc@openssl.com</a></td>
</tr>
<tr>
<td>TLS_RSA_WITH_3DES_EDE_CBC_SHA</td>
<td>DES-CBC3-SHA</td>
<td>3des-cbc</td>
<td>hmac-sha1, <a href="mailto:hmac-sha1-etc@openssl.com">hmac-sha1-etc@openssl.com</a></td>
</tr>
<tr>
<td>Protocol</td>
<td>Cipher Suite</td>
<td>Algorithm</td>
<td>HMAC Type</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------</td>
<td>-----------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>TLS_DHE_DSS_WITH_AES_128_CBC_SHA</td>
<td>DHE-DSS-AES128-SHA</td>
<td>aes128-cbc</td>
<td>hmac-sha1, <a href="mailto:hmac-sha1-etm@openssh.com">hmac-sha1-etm@openssh.com</a></td>
</tr>
<tr>
<td>TLS_DHE_DSS_WITH_AES_128_CBC_SHA</td>
<td>DHE-DSS-AES128-SHA</td>
<td>aes128-cbc</td>
<td>hmac-sha1, <a href="mailto:hmac-sha1-etm@openssh.com">hmac-sha1-etm@openssh.com</a></td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>AES128-SHA</td>
<td>aes128-cbc</td>
<td>hmac-sha1, <a href="mailto:hmac-sha1-etm@openssh.com">hmac-sha1-etm@openssh.com</a></td>
</tr>
<tr>
<td>TLS_RSA_WITH_RC4_128_SHA</td>
<td>RC4-SHA</td>
<td>arcfour128</td>
<td>hmac-sha1, <a href="mailto:hmac-sha1-etm@openssh.com">hmac-sha1-etm@openssh.com</a></td>
</tr>
<tr>
<td>TLS_DHE_DSS_WITH_AES_256_GCM_SHA384</td>
<td>DHE-DSS-AES256-GCM-SHA384</td>
<td><a href="mailto:aes256-gcm@opensh.com">aes256-gcm@opensh.com</a></td>
<td>hmac-sha2-512, <a href="mailto:hmac-sha2-512-etm@openssh.com">hmac-sha2-512-etm@openssh.com</a></td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>DHE-DSS-AES256-GCM-SHA384</td>
<td><a href="mailto:aes256-gcm@opensh.com">aes256-gcm@opensh.com</a></td>
<td>hmac-sha2-512, <a href="mailto:hmac-sha2-512-etm@openssh.com">hmac-sha2-512-etm@openssh.com</a></td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA256</td>
<td>DHE-RSA-AES256-SHA256</td>
<td>aes256-cbc</td>
<td>hmac-sha2-256, <a href="mailto:hmac-sha2-256-etm@openssh.com">hmac-sha2-256-etm@openssh.com</a></td>
</tr>
<tr>
<td>TLS_DHE_DSS_WITH_AES_256_CBC_SHA256</td>
<td>DHE-DSS-AES256-SHA256</td>
<td>aes256-cbc</td>
<td>hmac-sha2-256, <a href="mailto:hmac-sha2-256-etm@openssh.com">hmac-sha2-256-etm@openssh.com</a></td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_GCM_SHA384</td>
<td>AES256-GCM-SHA384</td>
<td><a href="mailto:aes256-gcm@opensh.com">aes256-gcm@opensh.com</a></td>
<td>hmac-sha2-512, <a href="mailto:hmac-sha2-512-etm@openssh.com">hmac-sha2-512-etm@openssh.com</a></td>
</tr>
<tr>
<td>TLS_DHE_DSS_WITH_AES_128_GCM_SHA256</td>
<td>DHE-DSS-AES128-GCM-SHA256</td>
<td><a href="mailto:aes256-gcm@opensh.com">aes256-gcm@opensh.com</a></td>
<td>hmac-sha2-256, <a href="mailto:hmac-sha2-256-etm@openssh.com">hmac-sha2-256-etm@openssh.com</a></td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</td>
<td>DHE-RSA-AES128-GCM-SHA256</td>
<td>aes256-cbc</td>
<td>hmac-sha2-256, <a href="mailto:hmac-sha2-256-etm@openssh.com">hmac-sha2-256-etm@openssh.com</a></td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA256</td>
<td>DHE-RSA-AES128-SHA256</td>
<td>aes128-cbc</td>
<td>hmac-sha2-256, <a href="mailto:hmac-sha2-256-etm@openssh.com">hmac-sha2-256-etm@openssh.com</a></td>
</tr>
<tr>
<td>TLS_DHE_DSS_WITH_AES_128_CBC_SHA256</td>
<td>DHE-DSS-AES128-SHA256</td>
<td>aes128-cbc</td>
<td>hmac-sha2-256, <a href="mailto:hmac-sha2-256-etm@openssh.com">hmac-sha2-256-etm@openssh.com</a></td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA256</td>
<td>AES128-SHA256</td>
<td>aes128-cbc</td>
<td>hmac-sha2-256, <a href="mailto:hmac-sha2-256-etm@openssh.com">hmac-sha2-256-etm@openssh.com</a></td>
</tr>
</tbody>
</table>

When a client first connects to a server, it starts a series of message exchanges, called the SSL/TLS handshake. During this exchange, the server authenticates itself to the client by sending its server certificate. A certificate is an electronic form that verifies the identity and public key of the subject of the certificate. (In SSL/TLS, the subject of the certificate is the server.) Certificates are typically issued and digitally signed by a trusted third party, the Certificate Authority (CA). A certificate contains the following information: the dates it is valid, the issuing CA, the server name, and the public key of the server. For information about certificates, see Managing Certificates.

A server generates two distinct but related keys: a public key and a private key. During the SSL/TLS handshake, the server sends its public key to the client. Once the client validates the certificate, it encrypts a random value with the public key and sends it to the server. The server decrypts the random value with its private key.

The server and the client exchange messages indicating that they are using the symmetric keys to encrypt further communications.

*Figure 1.2 SSL/TLS Handshake*
To avoid possible attacks in which HTTP or HTTPS connections are made to a web server and stay open much longer than they should be, Infoblox provides the `set connection_limit` and `show connection_limit` CLI commands that you can use to mitigate these attacks. In general, these attacks can result in the web server reaching its maximum number of concurrent connections, and thus denying connections from legitimate sources. You can use the CLI commands to limit the number of concurrent HTTP and HTTPS connections from a given client that corresponds to a particular IP address. For information about the CLI commands and how to use them, refer to the Infoblox CLI Guide.

Managing Certificates

About HTTPS Certificates

The NIOS appliance generates a self-signed certificate when it first starts. A self-signed certificate is signed by the subject of the certificate, and not by a CA (Certificate Authority). This is the default certificate. When your computer first connects to the NIOS appliance, it sends this certificate to authenticate itself to your browser. Because the default certificate is self-signed, your browser does not have a trusted CA certificate or a cached NIOS appliance server certificate (saved from an earlier connection) to authenticate the NIOS appliance certificate. Also, the hostname in the default certificate is `www.infoblox.co`
m, which is unlikely to match the hostname of your NIOS appliance. Consequently, messages appear warning that the certificate is not from a trusted certifying authority and that the hostname on the certificate is either invalid or does not match the name of the site that sent the certificate. Either accept the certificate just for this session or save it to the certificate store of your browser.

To eliminate certificate warnings, you can replace the default self-signed certificate with a different certificate that has the hostname of your NIOS appliance. The NIOS appliance supports X.509 certificates in .PEM format. After the initial login, you can do one of the following:

- Generate another self-signed certificate with the correct hostname and save it to the certificate store of your browser.
- Request a CA-signed certificate with the correct hostname and load it on the NIOS appliance. For more information, see 481716.
- When you receive the certificate from the CA, import it to the appliance, as described in 4817169.
- Download the certificate from a trusted CA, as described in 4817169.

Generating Self-Signed Certificates

You can replace the default certificate with a self-signed certificate that you generate. When you generate a self-signed certificate, you can specify the correct hostname and change the public/private key size, enter valid dates and specify additional information specific to the NIOS appliance. If you have multiple appliances, you can generate a certificate for each appliance with the appropriate hostname. You can generate a self-signed certificate using either the SHA-1 or SHA-256 (SHA-2) hash algorithm.

To generate a self-signed certificate:

1. Grid: From the Grid tab, select the Grid Manager tab -> Members tab -> member check box, and then click Certificates -> HTTPS Cert -> Generate Self-signed Certificate from the Toolbar. In a Grid, ensure that you select the Grid Master when generating a self-signed certificate.

2. In the Generate Self-Signed Certificate dialog box, complete the following:
   - Secure Hash Algorithm and Key Size: You can select SHA-1 and a RSA key size of 1024 or 2048. SHA-256 (SHA-2) can be selected together with a RSA key size of 2048 or 4096. The default value is SHA-256 2048.
   - Days Valid: Specify the validity period of the certificate.
   - Common Name: Specify the domain name of the NIOS appliance. You can enter the FQDN (fully qualified domain name) of the appliance.
   - Organization: Enter the name of your company.
   - Organizational Unit: Enter the name of your department.
   - Locality: Enter a location, such as the city or town of your company.
   - State or Province: Enter the state or province.
   - Country Code: Enter the two-letter code that identifies the country, such as US.
   - Admin E-mail Address: Enter the email address of the appliance administrator.
   - Comment: Enter information about the certificate.

3. Click OK.

4. If the appliance already has an existing HTTPS certificate, the new certificate replaces the existing one. In the Replace HTTPS Certificate Confirmation dialog box, click Yes. The appliance logs you out, or you can manually log out. When you log in to the appliance again, it uses the new certificate you generated.

Generating Certificate Signing Requests

You can generate a CSR (certificate signing request) that you can use to obtain a signed certificate from your own trusted CA. Once you receive the signed certificate, you can import it in to the NIOS appliance, as described in 4817169.

To generate a CSR:

1. Grid: From the Grid tab, select the Grid Manager tab -> Members tab -> member check box, and then click Certificates -> HTTPS Cert -> Create Signing Request from the Toolbar.

2. In the Create Certificate Signing Request dialog box, enter the following:
   - Secure Hash Algorithm and Key Size: You can select SHA-1 and a RSA key size of 1024 or 2048. SHA-256 (SHA-2) can be selected together with a RSA key size of 2048 or 4096. The default value is SHA-256 2048.
   - Common Name: Specify the domain name of the NIOS appliance. You can enter the FQDN of the appliance.
   - Organization: Enter the name of your company.
   - Organizational Unit: Enter the name of your department.
   - Locality: Enter a location, such as the city or town of your company.
   - State or Province: Enter the state or province.
   - Country Code: Enter the two-letter code that identifies the country, such as US.
   - Admin E-mail Address: Enter the email address of the appliance administrator.
   - Comment: Enter information about the certificate.

3. Click OK.

Uploading Certificates

When you receive the certificate from the CA, and import it to the appliance, the NIOS appliance finds the matching CSR and takes the private key associated with the CSR and associates it with the newly imported certificate. The appliance then automatically deletes the CSR.

If the CA sends an intermediate certificate that must be installed along with the server certificate, you can upload both certificates to the...
appliance. The appliance supports the use of intermediate certificates to complete the chain of trust from the server certificate to a trusted root CA. This eliminates intermediate certificate security warnings that appear when you open a web browser and try to connect to an Infoblox appliance.

To import a certificate:

1. Grid: From the Grid tab, select the Grid Manager tab -> Members tab -> member check box, and then click Certificates -> HTTPS Cert -> Upload Certificate from the Toolbar.
2. Navigate to where the certificate is located and click Open.
3. If the appliance already has an existing HTTPS certificate, the new certificate replaces the existing one. In the Replace HTTPS Certificate Confirmation dialog box, click Yes.

The appliance imports the certificate and logs you out. When you log in to the appliance again, it uses the certificate you imported.

Downloading Certificates

You can download the current certificate or a self-signed certificate, as described in 4817169 4817169.

To download a certificate:

1. Grid: From the Grid tab, select the Grid Manager tab -> Members tab -> member check box, and then click Certificates -> HTTPS Cert -> Download Certificate from the Toolbar.
2. Navigate to where you want to save the certificate, enter the file name, and then click Save.

About Client Certificates

You can generate client certificates for a Grid Master or a Grid Master candidate, and then send it to another server, such as a Hardware Security Module (HSM).

Generating a Client Certificate

To generate a client certificate:

1. Grid: From the Grid tab, select the Grid Manager tab.
   Grid Master Candidate: From the Grid tab, select the GridManager tab -> Members tab -> member check box.
2. From the Toolbar, click Certificates -> ClientCert -> GenerateClientCertificate, and select either RSASHA1 or RSASHA256.
   • If you are generating a certificate for an HSM group with SafeNet Luna SA 4 devices, you must select RSASHA1; and if the certificate is for an HSM group with SafeNet Luna SA 5 or Luna SA 6 devices, select RSASHA256.

The appliance displays a confirmation dialog after it generates the certificate. If a certificate had been previously generated, the appliance displays a dialog warning that if the previous certificate was registered with a server, then the new certificate must be registered with the server.

Viewing Client Certificates

To view the client certificates that were generated:

1. Grid: From the Grid tab, select the Grid Manager tab.
   Grid Master Candidate: From the Grid tab, select the GridManager tab -> Members tab -> member check box.
2. From the Toolbar, click Certificates -> Client Cert -> View Client Certificate, and select either RSASHA1 or RSASHA256.

The appliance displays the selected certificate.

Downloading Client Certificates

To download a client certificate:

1. Grid: From the Grid tab, select the Grid Manager tab.
   Grid Master Candidate: From the Grid tab, select the GridManager tab -> Members tab -> member check box.
2. From the Toolbar, click Certificates -> Client Cert -> Download Client Certificate, and select either RSASHA1 or RSASHA256.
3. Save the certificate.

About CA Certificates

If the CA sends an intermediate certificate that must be installed along with the server certificate, you can upload both certificates to the appliance. The appliance supports the use of intermediate certificates to complete the chain of trust from the server certificate to a trusted root CA. This eliminates intermediate certificate security warnings that appear when you open a web browser and try to connect to an Infoblox appliance.
When you configure two-factor authentication for smart card users, ensure that you upload the required CA certificates before you enable the certificate authentication service. For information about two factor authentication and how to configure it, see Defining the Authentication Policy. Only superusers and limited-access users with the required permissions can manage CA certificates. For information about admin permissions, see Administrative Permissions for Certificate Authentication Services and CA Certificates.

Uploading CA Certificates

To upload a CA-signed certificate:

1. Grid: From the Grid tab, select the Grid Manager tab.
2. Member: From the Grid tab, select the Grid Manager tab -> Members tab -> member check box.
3. Select Certificates -> Manage CA Certificates from the Toolbar.
4. In the CA Certificates editor, click the Add icon.
5. In the Upload dialog box, click Select and navigate to the certificate you want to upload.
6. Select the file and click Upload.

Note: NIOS can only upload certificates that are in PEM format. A PEM file can contain more than one certificate. For information about how to convert CA certificates to .PEM format, see 4817169.

Repeat the steps to add additional CA-signed certificates.

The CA Certificates dialog box displays the following information about the intermediate certificates:

- **Subject**: The name of the certificate.
- **Issuer**: The name of the trusted CA that issued the certificate.
- **Serial**: The serial number of the certificate.
- **Valid**: The validity period of the certificate.
- **Used by**: Displays SSL/TLS, when CA certificate is not used for certificate authentication, or CAS, when CA certificate is associated with a certificate authentication service.

You can also do the following:

- Select a certificate and click the Delete icon to delete it.
- Print the data or export it in .csv format.

Converting CA Certificates to PEM Format

NIOS can only upload certificates that are in PEM format. PEM files are Base64 encoded ASCII files. You can use OpenSSL to convert other certificate formats, such as P7B and DER, into PEM format.

You can run OpenSSL on Linux and Windows systems. For Linux, OpenSSL is pre-installed. For Windows, you can manually install an OpenSSL for Windows. For information about OpenSSL, visit its web site at [http://www.openssl.org/](http://www.openssl.org/).

To convert a P7B file to PEM format using OpenSSL:

1. Download and unzip the CA certificate file in P7B format.
2. Navigate to the directory where you unzip the CA certificate file.
3. Identify the PKCS7 directory.
4. Use the following OpenSSL command to convert the P7B file to PEM format:
   ```
   $ openssl pkcs7 -in xxxx.p7b -print_certs -out yyyy.pem
   where xxxx is the name of the P7B file and yyyy is the name of the converted PEM file.
   ```

To convert a DER file to PEM format using OpenSSL:

1. Download and unzip the CA certificate file in DER format.
2. Navigate to the directory where you unzip the CA certificate file.
3. Use the following OpenSSL command to convert the DER file to PEM format:
   ```
   $ openssl x509 -inform DER -outform PEM -in xxxx.cer -out yyyy.pem
   where xxxx is the name of the DER file and yyyy is the name of the converted PEM file.
   ```

About the Grid Manager Interface

Grid Manager provides an easy-to-use interface that simplifies core network services management. Its navigational tools enable you to quickly move through the application and retrieve the information you need. You can customize different elements in your workspace, and hide and display panels as you need them. It also provides different types of Help, so you can immediately access the information you need to complete your tasks.

Figure 1.3 illustrates the typical layout of Grid Manager. It identifies common elements of the interface and features that you can use:

Figure 1.3 Grid Manager Interface
System Messages
Grid Manager displays system messages at the top of the screen. In wizards and editors, it displays messages at the top as well.

Note: Some configuration changes require a service restart. Grid Manager displays a message whenever you make such a change. Click the Restart icon that appears in the message to restart services.

Security and Informational Banners
Grid Manager displays banner messages on the header and footer of the screen. Only superusers can publish the informational and security banner. There are two types of banners:

- Security Banner - Security banner indicates the security level of the Infoblox Grid. There are five security levels to choose from the Security list box. The available security levels are Top Secret, Secret, Confidential, Restricted, and Unclassified.
- Informational Banner - You can use the informational banner for multiple uses, such as to indicate whether the Infoblox Grid is in production or a lab system. You can also publish messages of the day.

For more information, see Configuring Security Level Banner and Configuring Informational Level Banner.

Breadcrumbs Navigation
Breadcrumbs navigation displays your path to the current page. It helps you keep track of your location in Grid Manager. You can click any of the links to get back to a previous page.

Global Search
Use Global Search to find data. Grid Manager searches the entire NIOS database for data that matches the criteria you specify. For additional information on Global Search, see Using Global Search.

Finder Panel
The Finder panel appears on all pages in Grid Manager. It provides the following tools:

- Smart Folders: Use smart folders to organize your data according to criteria that you specify.
- Bookmarks: Stores data that you have marked for easy retrieval.
- Recycle Bin: Stores deleted objects that you can either restore or permanently remove.
- URL Links: You can add, modify, and delete third party URL links of frequently used portals and destination pages.

You can resize, collapse, and expand the Finder panel.
Toolbar Panel

The vertical Toolbar panel provides easy access to commands. The Toolbar is available in all pages, except the Dashboard. Its content changes depending on the type of data displayed in the work area. You can resize, collapse, and expand the Toolbar panel.

Help Panel

The Help panel provides the following types of Help:

- **Help**: Expand this section to view information about the window currently displayed.
- **Documentation**: Expand this section to download the latest versions of the Infoblox Administrator Guide and Infoblox API Documentation.
- **Support**: Expand this section to view links to the Infoblox web site and Technical Support site.
- **About**: Expand this section to view information about the NIOS software version. You can resize, collapse, and expand the Help panel. In addition, each dialog box also provides a Help panel that contains information specific to the dialog box. You can expand and collapse the Help panel in dialog boxes as well.

Wizards and Editors

Grid Manager provides a wizard for every object that you can create. You use wizards to enter basic information required to create an object. If you want to configure additional parameters, you can then save the object and edit it. Note that all required fields are denoted by asterisks.

Your connection to Grid Manager may time out if a save operation takes longer than 120 seconds to complete. This can occur when multiple, complex operations are initiated by several users. It does not result in any data loss.

Tooltips

Tooltips display the function of each button. Hover your mouse over a button or icon to display its label.

Customizing Tables

Grid Manager uses dynamic tables to display information. You can customize tables by resizing columns, sorting the data, and selecting certain columns for display. Your settings remain active until you log out.

To resize columns in a table:

1. In the table, place your pointer on the right border of the header of the column you want to resize.
2. Drag the border to the desired width.

To sort the data displayed in a table, click the header title. You can click the header title again to reverse the sort order. Alternatively, you can do the following:

1. In the table, mouse over to a header title and click the down arrow key.
2. Select **Sort Ascending** or **Sort Descending**. To edit columns:
3. In the table, mouse over to a header title and click the down arrow key.
4. Select **Columns > Edit Columns**.
5. Do the following:
   - **Width**: Specify the width of the column in pixels. The minimum is five and the maximum is 999.
   - **Sorted**: Indicates whether the data in the column can be sorted
   - **Visible**: Click the check boxes of the columns you want to display, and clear the check boxes of those you want to hide.
6. Do one of the following:
   - **Click Apply** to apply your settings to the column.
   - **Click Cancel** to close the editor without saving your settings.
   - **Click Reset** to reset the settings to the default.

Grid Manager displays the selected column in the table.

To reorder columns in a table, drag and drop the columns to the desired positions.

Selecting Objects in Tables

In a table, Grid Manager displays data on multiple pages when the number of items to be displayed exceeds the maximum number of items that can be displayed on one page. Use the navigational buttons at the bottom of the table to page through the display.
You can select multiple rows in a table. For example, in a Windows browser, you can do the following to select multiple rows:

- Use SHIFT+click to select multiple contiguous rows.
- Use CTRL+click to select multiple non-contiguous rows.
- Click the check box in the table header to select all rows on a page, as shown in Figure 1.4.

When you click the select all check box in a table that contains multiple pages, only the rows on the current page are selected. Grid Manager displays a message that indicates the total number of selected rows on the page. You can click Select all objects in the dataset to select all rows in the entire table. When you select all rows in the table, Grid Manager displays a message to indicate that. You can then click Clear Selection to deselect the rows.

After you select all rows on a page, you can deselect a specific row by clearing the check box of the row. You can also click a row (not the check box) in the table to select the item and deselect the others.

In a table, when you select all the objects for deletion, the objects that are not deleted from the database remain in the table after the operation is completed.

*Figure 1.4 Select All in a Table*

---

**Modifying Data in Tables**

Infoblox provides inline editing for certain fields in some tables. You can use this feature to modify data directly in a table instead of going through an editor.

To update information in a table, you must have read/write permission to the data. When you enter or select a new value, the appliance validates the data format before saving the updated data.

To modify data in a table:

1. From any panel that supports inline editing, double click the row of data that you want to modify. The appliance displays the inline editing editor in the selected row, as shown in Figure 1.5.
2. Depending on the data type, enter the new data in the field or select an item from the drop-down list. Note that some fields are read-only.
3. Click Save to save the changes, or click Cancel to discard them.

*Figure 1.5 Inline Editing*
Finding and Restoring Data

Grid Manager provides tools for organizing and quickly retrieving your DNS, DHCP and IP address management data. The Finder panel, which appears on all pages in Grid Manager, provides tools for organizing your data. The Finder panel provides easy access to the following:

- **Smart Folders**: Contains a hierarchical list of smart folders that are available in My Smart Folders. For more information, see My Smart Folders.
- **Bookmarks**: Contains bookmarked objects, such as networks and IP addresses. For more information, see Using Bookmarks.
- **Recycle Bin**: Contains deleted objects that can be restored or permanently removed. For more information, see Using the Recycle Bin.
- **URL Links**: Contains a list of third party URLs that you previously added. You can add more URL links, and modify and delete existing URL links. For more information, see Managing Third Party URL Links.

In the Finder panel, you can expand and collapse these sections. To expand a section, click the + icon next to the header. To collapse a section, click the - icon.

In addition, Grid Manager also provides the following:

- Filters to customize data displays. For more information, see Using Filters and Using Quick Filters.
- Global Search to search the NIOS database for objects that match your criteria. For more information, see Applying Quick Filters.
- Go To function to quickly locate an object. For more information, see Using the Go To Function.

Using Bookmarks

The Bookmarks section displays objects for which you have created bookmarks. You can create bookmarks for objects such as networks, DNS zones, and admin groups. To bookmark an object, navigate to its page and click the Bookmark icon at the top of the page. If you have more than one network view, Grid Manager displays the name of the bookmark with the network view to which the object belongs. For example, when you bookmark IP address 10.128.0.10 in the default network view, Grid Manager displays the bookmark as default > 10.128.0.10. However, if you have only one network view, Grid Manager displays only the object name 12.128.0.10. If you create a bookmark before adding more network views, the bookmark name (without the network view) remains the same. You can rename the bookmark at anytime. You can create only one bookmark for each object, up to 500 objects. When your bookmarks are close to 500, you may want to remove some to create room for new ones.

You can do the following in Bookmarks:
• Access a bookmarked object
• Edit the name of a bookmark
• Delete a bookmark

To access a bookmarked object, click the name of the bookmark. Grid Manager displays the network view to which the bookmarked object belongs. For example, clicking on the bookmark of network 10.0.1/24 takes you to the network list view. You cannot access an object that has been deleted.

You can arrange the order of the bookmarked objects by dragging and dropping the objects in the **Finder** panel. To edit the name of a bookmark:

1. Mouse over to the bookmark.
2. Click the Edit icon.
3. Modify the name of the bookmark. Note that you cannot create multiple bookmarks with the same name.

To delete a bookmark:

1. Mouse over to the bookmark.
2. Click the Delete icon. Grid Manager removes the bookmark.

**Using the Recycle Bin**

The Recycle Bin section contains objects that you deleted. It provides a way to restore data where the deletion of the object (such as a network) could result in a major data loss.

You must enable the Recycle Bin in Grid Manager to store and restore deleted objects. For information about how to enable and disable the Recycle Bin, see [bookmark104](#). When you use the Recycle Bin, you can restore deleted objects to the active configuration. You can also permanently remove the objects from the Recycle Bin. If you do not enable the Recycle Bin, the appliance immediately removes objects from the database when you delete them using Grid Manager.

**Note:** When you upgrade to a new NIOS release, the appliance permanently deletes the objects from the Recycle Bin.

On a NIOS appliance, only superusers have permissions to fully manage the Recycle Bin. If you have limited-access permissions, you can view, restore, and permanently remove only the objects that you deleted.

For Cloud Network Automation, the Recycle Bin is not supported on the Cloud Platform Appliance. Only deletions perform on the Grid Master are stored in the Recycle Bin. Deleted objects can only be restored from the Grid Master. For information about Cloud Network Automation, see [Deploying Cloud Network Automation](#).

You can do the following in the Recycle Bin:

- View deleted objects
- Restore deleted objects
- Remove deleted objects
- Empty the Recycle Bin

**Enabling and Disabling the Recycle Bin**

To enable or disable the Recycle Bin:

1. From the **Grid** tab, select the **Grid Manager** tab, and then click **Grid Properties** -> **Edit** from the Toolbar.
2. In the **Grid Properties** Editor, select the General tab, and then complete the following:
   1. Select **Enable Recycle Bin** to enable the Recycle Bin
      or
      Deselect **Enable Recycle Bin** to disable the Recycle Bin.
3. Save the configuration and click **Restart** if it appears at the top of the screen.

**Viewing Objects in the Recycle Bin**

Grid Manager displays the short name of all deleted objects in the Recycle Bin. For example, the short names for hosts and resource records are their domain names, and the short names for fixed addresses and reservations are their IP addresses.

The Recycle Bin does not display all deleted objects; it can display up to 15 of the most recently deleted objects. When the Recycle Bin contains objects that are not displayed in the **Finder** panel or multiple objects that have the same name, the **Show All** button appears. Click the button to display the **Recycle Bin** dialog box that contains detailed information about each deleted object. When you have multiple deleted objects that use the same name, you may want to view detailed information about the deleted objects before taking any action. You can remove and restore selected objects and empty the Recycle Bin in the **Recycle Bin** dialog box.

You can do the following in the **Recycle Bin** dialog box:

- Sort the data in ascending or descending order by column.
- Use filters and the search function to look for specific objects. For information about filters, see [Using Filters](#)
Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters

Use the GoTo function to quickly find the data in the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Goto field and select the object from the possible matches.

To view detailed information about deleted objects:
1. In the Finder panel, expand Recycle Bin.
2. Click Show All.

Grid Manager displays the Recycle Bin dialog box that contains the following information for each object:

- **Name**: The short name of the object. For example, the short names for fixed addresses and reservations are their IP addresses.
- **Type**: The object type.
- **Parent/Container**: The parent object or parent container to which the object belongs.
- **Admin**: The admin name of the user who deleted the object.
- **Data**: The data that the object contains, if any.
- **NetworkView**: The network view to which the object belongs.
- **Time**: The time stamp when the object was deleted. To close the dialog box, click Close.

**Restoring Objects from the Recycle Bin**

You can restore deleted objects from the Recycle Bin only if you enable the Recycle Bin, and only if you select an object in the panel. You can restore only one object at a time. Deleted objects are stored in the Recycle Bin until you delete them or empty the bin.

To restore items from the Recycle Bin:
1. In the Finder panel, expand Recycle Bin.
2. Select the object you want to restore.
3. Click the Restore icon.

Grid Manager restores the object to its corresponding container or configuration. You can confirm the restoration by checking that the object does not appear in the Recycle Bin any longer, and that it is reestablished in the appropriate panel in the GUI.

**Deleting Objects in the Recycle Bin**

You can permanently delete individual objects in the Recycle Bin only if the Recycle Bin is enabled. To delete objects in the Recycle Bin:
1. In the Finder panel, expand Recycle Bin.
2. Select the object you want to delete.
3. Click the Delete icon.
4. Click Yes to delete the object.

**Emptying the Recycle Bin**

You can permanently delete the contents of the Recycle Bin, if enabled. Only superusers can empty the Recycle Bin. Because the Recycle Bin can grow large, you can periodically empty the Recycle Bin to free up disk space.

To empty the Recycle Bin:
1. In the Finder panel, expand Recycle Bin.
2. Click Empty.
   - Grid Manager displays the ConfirmEmptyRecycleBin dialog box to confirm that you wish to empty the Recycle Bin.
3. Click Yes.

**Managing Third Party URL Links**

In the URL Links section, you can add the URL links of frequently used third party portals and destinations.

**Adding URL Links**
1. In the Finder panel, expand URL Links.
2. Click Add.
3. In the URL Configuration dialog box, complete the following:
   - **URL**: Enter the URL of the destination characters. When you enter the URL, the appliance validates the entry. You cannot save the entry if the URL is not in a valid format.
   - **Name**: Enter a name that represents the portal or site of the URL.
   - **Set as global parameter**: This field appears only if you log in as a superuser. Select this check box to make the URL link globally available to all users.
Modifying URL Links

To modify the information you entered for an existing URL link:

1. In the Finder panel, expand **URL Links**.
2. Hover your mouse over the URL you want to modify, and then click the Edit icon.
3. In the **URL Configuration** dialog box, modify the information as described in **Adding URL Links**.

Deleting URL Links

To permanently delete an URL link:

1. In the Finder panel, expand **URL Links**.
2. Hover your mouse over the URL you want to delete, and then click the Delete icon.
3. In the **Delete URL Link** dialog box, click **Yes**.

Using Filters

You can control the amount and the kind of data displayed in a specific panel by adding filter criteria. When you add filter criteria, the appliance screens the data based on your filter rules and displays only the information that matches the rules. To narrow your search for specific information, you can add up to 10 filter rules. In some panels, such as the DHCP Networks tab, you can switch between viewing information with and without the filter criteria by toggling the filter on and off. You can save filter criteria as quick filters so you can reuse the same filter rules to obtain updated information without redefining them each time you log in to the appliance. For information about quick filters, see **Using Quick Filters**.

You can also use filters to find objects that have failed an operation. When you try to modify multiple objects with the same extensible attribute, the appliance may not modify all of the selected objects. For information, see **About Extensible Attributes**. For example, after you modify the extensible attribute “Building” with new value “West”, you can find the objects that are not updated by defining a filter with “Building” “does not equal” “West”.

Depending on the filter criteria, you can use different filter operations to narrow down your search results. Grid Manager supports the following filter operations based on your selected filter criteria:

- equals: Defines a specific value for a selected filter criterion
- does not equal: Defines a selected filter criterion that does not equal a specific value
- begins with: Specifies a beginning value for a selected filter criterion
- does not begin with: Specifies a selected filter criterion that does not begin with a specific value
- has a value: Specifies a selected filter criterion that contains a value
- does not have a value: Specifies a selected filter criterion that does not contain a value
- belongs to: Defines a selected filter criterion that belongs to a specific parent object
- Inheritance State equals: Specifies a specific inheritance state

To use a filter:

1. In a panel, click **Show Filter** to enable the function.
2. In the filter section, complete the following:
   - In the first drop-down list, select a field such as an object name, comment, or an extensible attribute (fields with a gray background) as the filter criterion. Grid Manager displays only the supported fields.
   - In the operator drop-down list, select an operator for the filter criterion. Depending on what you select in the first filter field, this list displays the relevant operators for the selection. The operator **Inheritance State equals** is displayed only when you select an inheritable extensible attribute from the **Type** drop-down list. This operator is not displayed if the extensible attribute is not inheritable.
   - In the value field, enter or select the attribute value for the first filter field. Depending on what you select for the first two filter fields, you can either enter a value or select an attribute from a drop-down list. For example, if you select an extensible attribute in the first filter field, you can enter the attribute value here. If you select an inheritable extensible attribute from the **Type** drop-down list, and select **Inheritance State equals** in the operator drop-down list, the value field displays a drop-down list with these values: **Inherited** and **Overridden/No Parent**. When you select **Inherited**, extensible attributes that are inherited by the descendants are listed. When you select **Overridden/No Parent**, extensible attributes which are overridden or do not have a parent are listed.
3. Optionally, click the + icon to add another filter rule. You can add up to 10 filter rules.
4. Click **Apply** to apply the rules
   or
   Click **Reset** to clear the filter criteria.

To view information with or without the filter criteria:

- Click **Toggle Filter On** to apply filter criteria to the displayed data. Grid Manager displays only the filtered data in the panel.
Using Quick Filters

A quick filter saves filter rules that you define in a specific panel. You can reuse a quick filter to find updated information in a panel without specifying the same rules each time. Superusers can define quick filters and share them with local users. Limited-access users can only create quick filters for their own use. You can create up to 10 global and 10 local quick filters in each panel that supports filters. For information about filters, see Using Filters.

The appliance supports the following quick filters:

- **System quick filters**: These are predefined filters. You cannot modify the criteria of these filters. System quick filters are prefixed with \[S\] in the quick filter list. Infoblox currently supports the following system quick filters in the DNS data panels:
  - **All Forward Mapping Zones**: This quick filter displays all forward mapping zones in lexicographical order.
  - **All Reverse Mapping Zones**: This quick filter displays all IPv4 and IPv6 reverse mapping zones in numerical order. The appliance displays IPv4 zones before IPv6 zones.
  - **All IPv4 Reverse Mapping Zones**: This quick filter displays only the IPv4 reverse mapping zones in numerical order.
  - **All IPv6 Reverse Mapping Zones**: This quick filter displays only the IPv6 reverse mapping zones in numerical order.
  - **RPZ Logs**: This quick filter displays only the RPZ syslog messages in CEF format. This option is displayed only in the Syslog when RPZ license is enabled.

- **Global quick filters**: Only superusers can define global quick filters. You can make global filters available to all users. Limited-access users can use global quick filters, but they cannot modify them. Global filters are prefixed with \[G\] in the filter list.

- **Local quick filters**: Limited-access users can create local quick filters for their own use. You cannot share local quick filters with other users in the Grid. Local filters are prefixed with \[L\] in the filter list.

**Note**: In the default DNS zone view, the appliance displays forward mapping zones first, followed by IPv4 reverse mapping zones, and then IPv6 reverse mapping zones.

Adding Quick Filters

1. In a panel that supports filters, click Show Filters.
2. In the filter section, define filter criteria for the quick filter, as described in Using Filters.
3. Click Save.
4. In the Save Quick Filter dialog box, complete the following:
   - **Name**: Enter a name for the quick filter. The name must be 20 characters or longer. Ensure that you use a unique name for each quick filter in a particular filter category. For example, you can use the same filter name for both a global and local filter, but you cannot do so for two local filters.
   - **Set as a global quick filter**: This displays only if you log in as a superuser. Select this check box to make the quick filter globally available to all users.
5. Save the configuration.

The appliance adds the quick filter to the quick filter drop-down list in the specified panel.

Modifying Quick Filters

1. In a panel that supports filters, click Show Filters, and then select the quick filter you want to modify from the Quick Filter drop-down list.
2. In the filter section, click the Edit icon next to the filter name.
3. Modify the filter criteria, as described in Using Filters.
4. Click Save.
5. In the Save Quick Filter dialog box, you can click Save to save the modified filter criteria under the same quick filter name. You can also modify the quick filter name, as described in Modifying Quick Filters, and save the entry as a new quick filter.
6. Save the configuration.

Applying Quick Filters

1. In a panel that supports filters, click Show Filters, and select the quick filter from the Quick Filter drop-down list.
2. Based on the filter criteria, the appliance displays the filtered information in the panel. The selected quick filter remains active in the panel until you select another quick filter.

Turning Off Quick Filters

You can do one of the following to turn off a quick filter:

- Select None from the quick filter drop-down list.
Using Global Search

You can use the global search function to search the entire NIOS database for data that matches a specific value and filter criteria. You can define filter criteria and enter applicable search values to refine the search. Grid Manager supports regular expressions in global search. Grid Manager can display up to 500 search results. When search results exceed 500, a warning message appears and you may want to refine your search. Search results remain in the Search dialog box until you reset the search parameters or log out of Grid Manager. You can search for DNS zones and resource records that contain IDNs. For information about IDNs, see Support for Internationalized Domain Names.

Based on your search requirements, you can choose to perform a basic search or an advanced search.

A basic global search provides a faster way to locate frequently searched results using one specific filter criterion. It is designed to handle a large amount of data in an efficient manner. Supported filtering objects are DNS name (FQDN or CNAME only), DUID, IP address and MAC address. This is the recommended global search method if you have a large data set and only need to search by a single filter criterion.

An advanced global search allows you to perform complex searches by defining multiple filter criteria. You can add up to 10 filtering rules. You can also include existing extensible attributes for the matching objects.

Note that if a search result contains duplicate records, the appliance displays only one record and discards others. For example, if the canonical name matches an alias name, the appliance displays only one CNAME record in the result.

Note: Depending on the size of your database, global search may take a long time to complete. Grid Manager times out when queries or searches take longer than 120 seconds. To expedite searches, use filters to refine the search criteria. You can also use basic global searches if you have a large data set and you only need to search by a single filter criterion.

You can also do the following in the Results table:

- Click the Open icon to view detailed information of the matching object.
- Click the Edit icon to edit the matching object information. For information, see Editing Matching Objects in Search Results.
- Click the Extensible Attributes icon to edit the value of the respective extensible attribute. For information, see Editing Multiple Extensible Attributes in Search Results.
- Click the Export icon to export the data displayed in the Results table.
- Click the Print icon to print the data displayed in the Results table.

To perform a global search:

1. Click the Global Search icon on the navigation bar.
   By default, the appliance opens the Basic tab of the Search dialog box.
2. Do one of the following:

   If you want faster search results and you can search by DNS name, DUID, IP address, or MAC address, do the following in the Basic tab:

   Include Network Insight Devices and Interfaces: This appears only when you have the Network Insight license installed. Select this check box to include devices and interfaces discovered through Network Insight. Note that it might take longer than expected for the appliance to return results for these objects. The setting is saved between user sessions.

   - Choose Filter: Select a value from the drop-down list. You can explicitly search by DNS name (FQDN or CNAME only), DUID, IP address, or a MAC address. Note that you can apply only one filter at a time.
   - Choose Operator: Select an operator for the filter criterion. Depending on what you select in the first filter field, this list displays the relevant operators for the selection. Possible values include equals, begins with, and contains. For example, if you choose a DNS Name filter, contains is the only applicable operator.
   - In the value field, enter the value that you want your search results to match. For example, if you want to search for hostnames that contain "Infoblox," enter Infoblox in this field. You can also specify the value of an inheritable extensible attribute. You can use regular expressions in the search value. For information, see Regular Expressions.
   - In the Type drop-down list, select an object type, comment, or an extensible attribute (fields with a gray background) as the filter criterion. Grid Manager displays all the supported fields in the drop-down list. The default is Type. Grid Manager searches all objects when you use the default. You can narrow down the search and improve the search performance by selecting an object type. Extensible attributes are displayed with a gray background.
   - In the operator drop-down list, select an operator for the filter criterion. Depending on what you select in the first filter field, this list displays the relevant operators for the selection. The operator InheritanceStatequals is displayed only when you select an inheritable extensible attribute from the Type drop-down list. This operator is not displayed if the extensible attribute is not inheritable.
In the value field, enter or select the attribute value for the first filter field. Depending on what you select for the first two filter fields, you can either enter a value or select an attribute from a drop-down list. For example, if you select an extensible attribute in the first filter field, you can enter the attribute value here. If you use the default Type in the first filter field, you can select an object or record type from the drop-down list. The default is ALL. Grid Manager searches all object types when you use the default. If you select an inheritable extensible attribute from the Type drop-down list, and select Inheritance State equals in the operator drop-down list, the value field displays a drop-down list with these values: Inherited and Overridden/No Parent. When you select Inherited, extensible attributes that are inherited by the descendants are listed. When you select Overridden/No Parent, extensible attributes which are overridden or do not have a parent are listed.

- Optionally, click the + icon to add another filter. You can add up to 10 filter rules.
- **IncludeExtensibleAttributesValues**: Select this check box to include extensible attributes in the search results for the matching objects. Once selected, this configuration affects all future searches for the current user. Note that it might take longer for the search results to appear if there are a large number of extensible attributes associated with the matching objects.

**Note:** You can save each search that contains multiple filter criteria as a quick filter for future use. For information about quick filters, see Using Quick Filters.

3. Optionally, you can click Reset to clear the search results and start a new search. You can also click the Refresh icon to refresh the search results.

Grid Manager stores the search results until you reset the search parameters or log out.

4. After you finish defining filters, click Search or press Enter.

In the Results table, Grid Manager displays the following information:

- **Name**: The name of the matching object. This field displays the name of the matching object and the path to the matching object if the object is a network or an IP address. You can click the link to open, view, and edit the object.
- **Type**: The type of the matching object. For example, bulk host, NS record, forward-mapping authoritative zone, or network container.
- **Matched Property**: The attribute or property of the matching object. For example, if the search value matches the email address that corresponds to a hostname, this field displays Email. If the search value matches the DNS view of a resource record in a DNS zone, this field displays DNS View/FQDN.
- **MatchedValue**: The value of the matching object. For example, if an IP address contains the search value, this field displays the IP address. If a hostname contains the search value, this field displays the hostname.
- **IPAddress**: The IP address of the matching object. When you click the IP address link, Grid Manager displays the corresponding IP address panel from which you can view detailed information.
- **Comment**: Comments that were entered for the matching object.
- **Site**: Values that were entered for the matching object.

**Note:** If you have selected to include extensible attribute values, you can select the corresponding columns to be displayed in the search results. Extensible attribute columns are hidden by default.

### Editing Matching Objects in Search Results

Grid Manager displays search results in the Results table. You can open and view detailed information about an object. You can also edit the properties of a selected object.

To edit an object in the Results table:

1. In the Results table, select the object check box.
2. Click the Open or Edit icon. You can also click the link of an object if Grid Manager displays the path. Grid Manager displays the object in the corresponding editor depending on the type of object you selected.
3. Edit the properties of the object in the editor.
4. Save your changes.

### Deleting Matching Objects in Search Results

You can delete one or multiple matching objects in the search Results table. To delete a matching object:

1. In the Results table, select the object check box. You can delete multiple objects.
2. Click the Delete icon.
3. In the Delete Confirmation dialog box, click Yes.

Grid Manager deletes the selected objects from the database. Most deleted objects are stored in the Recycle Bin. For information, see Using the Recycle Bin

You can print search results. You can also export search results in CSV (comma separated value) format. For information, see About CSV Import and Exporting Displayed Data.

### Editing Multiple Extensible Attributes in Search Results

You can edit one or multiple extensible attributes of the matching objects in the search Results table using the Multi-Select Edit Extensible Attribute...
es editor. When you change multiple extensible attribute values for selected objects, the values of all selected extensible attributes will be updated.

To edit multiple extensible attributes:

1. In the Results table, select the object check box. You can edit multiple extensible attribute values.
2. Click the Extensible Attributes icon.
3. In the Multi-Select Edit Extensible Attributes editor, click on the Value column to edit the value of the respective extensible attribute. For information about which values you can edit, see Editing Multiple Extensible Attribute Values.

Using the Go To Function

You can use the Go To function to quickly locate an object, such as a network or a DNS zone. With the autocomplete feature, you can just type the first few characters of an object name in the Go to field and select the object from a list of possible matches. You can also enter the entire object name, and then click Go to locate a specific object.

To use the Go to function:

1. From a selector, enter the first few characters of the object name in the Go to field. Grid Manager displays up to ten possible matches in a drop-down list.
2. Click the object from the drop-down list, or use the up and down arrow keys to select the object and then press Enter. Grid Manager completes the operation based on the selected object.

About Tasks

When you perform a task, such as adding a DNS zone or modifying a DHCP range, you can execute it immediately or schedule it for a future date and time, depending on your permissions. For information about how to schedule a task, see Scheduling Tasks. Certain tasks, scheduled or not, may be subject to approvals if approval workflows are defined for specific admin groups. For information about how to define submitters and approvers for an approval workflow, see Configuring Approval Workflows.

Note that not all tasks can be scheduled or routed for approval. For a list of supported objects, see 4817222 4817222.

When you schedule a task or submit it for approval, consider the following:

- The appliance cannot execute a scheduled or approval task that is associated with an extensible attribute, if you delete the extensible attribute after you have scheduled the task or submitted it for approval. For information about extensible attributes, see About Extensible Attributes.
- The appliance cannot execute, reschedule, or delete a task that is associated with a child object (such as a DHCP range) if you delete the parent object (such as a network) after you have scheduled the task or submitted it for approval.
- There are certain guidelines about scheduled and approval tasks when you upgrade the software, back up the database, and restore data. For information, see 4817222.

Viewing Tasks

The appliance displays scheduled tasks and approval tasks in the Task Manager tab of Grid Manager. Scheduled tasks are those with scheduled time listed and approval tasks contain approval status. A task can also be scheduled and queued for approval at the same time. By default, all completed and rejected tasks are displayed in Task Manager for up to 14 days before they are removed from the list. You can configure how long the completed and rejected tasks are displayed in Task Manager using the CLI command set delete_tasks_interval. For more information about the CLI command, refer to the Infoblox CLI Guide.

The appliance logs all tasks in the audit log and associates each with a task ID. By default, Grid Manager sorts tasks by Task ID in Task Manager. You can view tasks that you are allowed to see based on your permissions. For information about admin permissions, see About Administrative Permissions.

To view tasks:

1. From the Administration tab, select the Workflow tab -> TaskManager tab.
2. Grid Manager displays the following information for each task:
   - **Task ID**: The ID associated with the task. The appliance assigns an ID to a task in chronological order. By default, the appliance sorts tasks by Task ID.
   - **Type**: Indicates key information about certain types of executing/executed jobs. The Type column lists values for Port Control and for Object Change tasks undertaken by Grid Manager or submitted by Grid Manager for approval by the administrator.
   - **AffectedObject**: The name or value of the object that is associated with the task. For example, if the task involves an A record, this field displays the domain name of the record. If it is a fixed address, it displays the IP address of the fixed address.
   - **ScheduledTime**: The date, time, and time zone when the appliance executes the task.
   - **SubmittedTime**: The date, time, and time zone when the task was submitted.
   - **Submitter**: The username of the admin who scheduled or submitted the task.
   - **TicketNumber**: For an approval workflow, this number may be entered by the submitter to associate the task with a help desk ticket number or a reference number.
   - **SubmitterComment**: Comments entered by the submitter.
   - **ApprovalStatus**: The current approval status. Possible values are Approved, NotApplicable, Pending, and Rejected.
   - **ExecutionStatus**: The execution status of the task. Possible values are Completed, Failed, Pending, and Executing.
   - **ExecutedTime**: The date, time, and time zone the task was executed.
   - **AssociatedTask**: (hidden by default) Applies to Port Configuration tasks. If a port configuration task is dependent on an object change task (such as a new Fixed Address or an edit to an existing object), this could will show the Task ID value for the associated object.
change task.

- **Action**: The operation the appliance performs in this task. The can be: Add, Modify, Delete, NetworkDiscovery, Lock/UnlockZone, or RestartServices.
- **TaskDetails**: Detailed information about the task. This message also appears in the audit log.
- **Approver**: The username of the admin who has approved this task.
- **ApproverComment**: Comments entered by the approver.
- **ObjectType**: The object type. For example, the appliance can display A Record or Fixed Address.

You can do the following in the Task Manager tab:

- Sort the tasks in ascending or descending order by column, except for Task Details.
- Use filters and the search function to look for specific values.

**Note**: You cannot use the search function to search for approval or execution status. Use filters to search for these values.

- Create a quick filter to save frequently used filter criteria. Grid Manager provides the following default quick filters that you can select from the Quick Filter drop-down list: Pending Approvals, Rejected Tasks, and Scheduled Tasks. For more information, see Using Quick Filters.
- Export and print the information in the table.
- Control the display of information in the panel by toggling between a single-line view and a multi-line view.
- Reschedule a task, cancel a scheduled task, or execute a task immediately.
- For approvers, select a task and click the Approve icon to approve the task, or click the Reject icon to disapprove the task. You can also reschedule the task while approving it.

**Note**: If you have multiple pages of tasks in Task Manager, you can select multiple tasks on the current page for approval or disapproval. If you click the Select all objects in this dataset link to select all the tasks in the dataset, the Approve and Reject icons are disabled and you cannot approve or reject any task.

### Using the Task Manager Action Menu

The Task Manager page provides an Action icon column with a series of menu options for features related to grid Manager tasks to manage task execution, scheduling and approval. Menu choices change based upon the context and the current state of tasks in the table; features available in the Action menu include the following:

![Task Manager Action menu](image)

- **(Applies only with Network Insight) Approve and Reject**: Enables admins to approve or reject a pending job; rejecting a job immediately cancels it.
- **AssociatedTask** (applies only with port configuration tasks): Choosing this option opens the object change task, if any, for the currently selected port configuration task.
- **ExecutionLog**: Opens a completed task's execution log window. The Execution Log lists the complete communications sequence sent to a device to perform a port control task.
- **ExecuteNow**: Force a selected pending task to execute immediately.
- **Re-execute**: Allows you to re-run the selected task. Combined with the Execution Log, this process can aid in troubleshooting a failed port control task.
- **Reschedule**: Opens the Reschedule window for the selected task. To immediately execute this task, click Now. Or, in the Reschedule panel, click Later, and then specify a date, time, and time zone. You can reschedule the task if you have the applicable permissions. Click Save to commit the changes.
- **Delete**: Deletes the pending task.
- **View**: Opens the Task Viewer to the currently selected task. For related information, see Using the Task Viewer to View Job Logs and Approve Jobs.

### Supported Objects for Scheduled and Approval Tasks

- DNS zones (authoritative, forward, stub, and delegated)
- DNS views
- DNS resource records (except SOA records)
• Import resource records to DNS zones
• Lock and unlock DNS zones
• Hosts
• Bulk hosts
• Roaming hosts
• Shared records
• Shared record groups
• IPv4 and IPv6 networks
• IPv4 and IPv6 network containers
• IPv4 and IPv6 shared networks
• IPv4 and IPv6 DHCP ranges
• IPv4 and IPv6 reserved ranges
• IPv4 and IPv6 fixed addresses
• IPv4 reservations
• DHCP fingerprints
• IPv4 DHCP filters (MAC, option, NAC, relay agent, and DHCP Fingerprint)

**Note:** Only IPv4 MAC filters support approval workflows.

• IPv4 MAC address filter items
• Conversion of IPv4 and IPv6 static and dynamic leases
• Microsoft objects that are supported by NIOS
• Load balancer related objects
• DNS64 Synthesis Groups
• All IPAM tasks except CSV imports
• Response Policy Zones
• Response Policy records

You can also schedule the following operations or create approval workflows for them:

• Network Discovery
• Device Discovery
• VM Discovery
• Port Control provisioning tasks for setting Admin Status, VLAN assignments, and a Description;
• Defining infrastructure device port reservations for the following IPAM/DHCP objects:
  • IPv4 Reservations
  • IPv4/IPv6 Fixed Addresses
  • Hosts
  • Grid Members
  • IPv4 and IPv6 Networks
• Service restarts (for scheduled tasks only)

**Note:** Service restarts are not subject to approvals.

---

**Guidelines for Upgrading, Backing Up, and Restoring Data**

You should take into consideration the impact on scheduled and approval tasks when you perform any of the following:

• When you upgrade from previous releases to NIOS 6.7 and later, the appliance converts all valid punycode data to IDNs for DNS resource records and DNS zones. When you have a fresh installation of NIOS 6.7 and later, the appliance converts all valid punycode data to IDNs for DNS zones only. It retains punycode data for resource records.
• Upgrade the NIOS software: In a full upgrade, all scheduled and approval tasks are deleted. In a lite upgrade, scheduled and approval tasks are not deleted.
• Back up the NIOS database: All scheduled and approval tasks are backed up for troubleshooting purpose.
• Restore the database: Scheduled and approval tasks are not restored.
• Promote a Grid member to a Grid Master: After the promotion, all scheduled and approval tasks that are past due are executed immediately.
• Revert the NIOS software image: After the revert, all scheduled and approval tasks that are past due are executed immediately.
• Restore data from the Recycle Bin: To restore a deleted parent object (such as a network) that contains a child object (such as a DHCP range) associated with a scheduled or approval task, you must first delete the scheduled or approval task for the child object.

**Scheduling Tasks**

You can schedule tasks, such as adding DNS zones, modifying fixed addresses, and restarting services, for a future date and time. The scheduling feature is useful when you want to add, modify, or delete a record, or schedule a network discovery at a desired date and time. Using this feature, you can streamline your day-to-day operations. For example, you can schedule the deletion of records that you use for testing when the test time is up. You can also reassign an IP address to a fixed address when the location of the server to which the fixed address is assigned changes from one network to another. You can schedule the addition, modification, and deletion of certain objects. For a list of the supported objects, see [Supported Objects for Scheduling and Approval Tasks](#).
Depending on your permissions and the admin group to which you belong, your scheduled tasks may be subject to approvals by other admins in your organization. You may or may not receive email notifications about the status of your scheduled tasks depending on the configuration of the approval workflows. Approvers can reschedule your tasks after they have approved the tasks, if they have scheduling permissions. When you schedule and submit a task, you may need to enter a ticket number associated with the task or a comment about the task. For more information about approval workflows, see Configuring Approval Workflows.

Only superusers can view, reschedule, and delete all scheduled tasks. Limited-access admins can reschedule and delete only their scheduled tasks. If your scheduled tasks require approvals, the approvers who have scheduling permissions may reschedule your tasks to a different date and time after they have approved the tasks. Depending on your admin permissions, there are certain scheduled and approval tasks that you may or may not be able to perform. For more information, see Supported Tasks for Different Admin Groups.

The appliance sends email notifications to local admins, except for those who do not have email addresses, when email notification is enabled for the admins and any of the following happens:

- A superuser schedules a task, and another superuser reschedules or deletes the task.
- A limited-access admin schedules a task, and a superuser reschedules or deletes the task.
- A superuser or a limited-access admin schedules a task, and the task fails.
- An admin is configured to receive notifications based on the configuration of an approval workflow. For information about approval workflows, see Configuring Approval Workflows.

Superusers can also grant scheduling permissions to other admin groups. When the scheduling permission is added or inherited from an admin role, limited-access admin groups can schedule tasks. For information, see Administrative Permissions for Network Discovery.

### Scheduling New IPAM/DHCP Objects and Associated Port Configurations

Specific IPAM/DHCP object types support scheduling of Port Configuration tasks as part of their object definition:

- New IPv4 and IPv6 Networks;
- IPv4 Reservations;
- Fixed IPv4 Addresses;
- Fixed IPv6 Addresses;
- Hosts;
- Infoblox Grid Members (including HA Pairs; discussed in the sections beginning in Adding Grid Members).

For all of these object types, you can click a Schedule for Later button at any step in the Wizard to commit the currently defined settings for the new object to a new Grid Manager task. For example, consider creating a new IPv4 network. After defining the IP address for the new network, you simply wish to create it and not to define any further configurations. Click Schedule for Later to skip the intervening Wizard steps and display the final Scheduling page of the Wizard, an example of which appears in Figure 1.7.

**Figure 1.7 Create Network Schedule for Later page**

![Create Network Schedule for Later page](image)

1. To create the new object immediately, select Now and click Save & Close.
2. You can choose to have Grid Manager create the object at a later time. To do so, select Later. Choose a Selected time by entering or selecting a Start Date (click the calendar icon to choose a calendar date) and a Start Time (click the clock icon to choose a specific time in fifteen minute increments), and choose a Time Zone.

When you step through the entire Wizard process (without clicking Schedule for Later) and if you also define port configuration settings, the object creation wizards provide a final Scheduling page with separate scheduling definitions, for the object and for the object's port configuration, as shown in Figure 1.8.

**Figure 1.8 Scheduling Create Object and Port Configuration**
The final step for creating the Network, Fixed Address, Host, or IP reservation is to define when the task executes, including associated port control definitions. The port configuration is performed in a separate task, defined on the same wizard page. The port configuration task can be done at the same time that Grid Manager provisions the object, or may be scheduled for a later time.

1. To create the new object immediately, select **Now**.

   By selecting Now, no task is created by Grid Manager and it simply creates the object. The completed object creation appears in the audit log (for related information, see the Viewing Tasks). Grid Manager creates a task for object creation only when you use **Schedule for Later**. Also, all port configuration and network provisioning instances create a new task under the Task Manager.

2. You can instruct Grid Manager to create the network at a later time. To do so, select **Later**. Choose a **Selected time** by entering or selecting a **Start Date** (click the calendar icon to choose a calendar date) and a **Start Time** (click the clock icon to choose a specific time in fifteen minute increments), and choose a **Time Zone**.

3. Port configuration and network provisioning tasks can be synchronized to take place at the same time as the creation of the new object under IPAM/DHCP; if so, keep the **At same time as above** option.
   
   a. You can also schedule the task at a different time. To do so, select **Later** (under **Port Configuration**). Choose a **Selected time** by entering or selecting a **Start Date** (click the calendar icon to choose a calendar date) and a **Start Time** (click the clock icon to choose a specific time in fifteen minute increments), and choose a **Time Zone**.

   The Port Configuration provision cannot take place at a schedule time or date before the associated object creation. Object creation must successfully complete before its associated port configuration task begins.

4. Click **Save & Close** to complete the configuration.

---

**Note:** Port configuration tasks (or any operation that queries for or changes device configurations through Grid Manager, including Discovery) are subject to a feature called Blackout Periods, which are defined elsewhere in Grid Manager. Blackouts are a scheduled feature that instructs Grid Manager not to perform Discovery operations and Port Control/provisioning operations on the managed network at specified times, days and dates. See the section **Defining Blackout Periods** for details.

---

**Scheduling Creation of new IPv4/IPv6 Networks and Associated Device Provisioning**

Defining new IP networks in Grid Manager supports scheduled Network Provisioning tasks on discovered and managed infrastructure devices as part of their object definition:

- Provisioning IPv4 networks
- Provisioning IPv6 networks

These networks are managed on the IPAM and DHCP pages (unless the network is excluded from DHCP), with the difference that Network Insight provisions the network directly on the specified router or switch-router. You may define new networks under IPAM and under DHCP as one scheduled task, and may provision those networks on devices that are discovered and managed under Network Insight, as another scheduled task.

Both tasks may be separately scheduled. They can take place immediately; the network is created first, then the network is provisioned on the device, along with the necessary device configuration, which Grid Manager also handles using the required CLI credentials; or either or both tasks may be scheduled for a later time.

The scheduled IPv4 or IPv6 network must be created under IPAM or DHCP in Grid Manager before scheduled device configuration or provisioning of networks on those devices can take place.

When you define a new network under IPAM or DHCP, you can click **Schedule for Later** in any Wizard page to skip further configuration in the
Wizard and commit the network settings to Grid Manager. If you do not want to provision the network, clicking Schedule for Later will display a shorter scheduling page:

Figure 1.9 Create Network Schedule page (After clicking Schedule for Later)

In cases of this type, you schedule or execute only a single task: creating the new network under DHCP/IPAM. No network provisioning task takes place.
When you provision the network without clicking Schedule for Later, the wizard provides a final Scheduling page with an expanded set of two task schedules as shown in Figure 1.10:

Figure 1.10 Scheduling Add Network and Network Provisioning Tasks

1. To immediately create the new network, you can select Now.
2. You can choose to have Grid Manager create the network at a later time. To do so, select Later. Choose a Selected time by entering or selecting a Start Date (click the calendar icon to choose a calendar date) and a Start Time (click the clock icon to choose a specific time in fifteen minute increments), and choose a Time Zone.
3. The Network Provisioning task can be synchronized to take place at the same time as the creation of the new network under IPAM/DHCP; if so, keep the At same time as above option.
4. You can also provision the network onto the device at a differently scheduled time. To do so, select Later (under Network Provisioning). Choose a Selected time by entering or selecting a Start Date (click the calendar icon to choose a calendar date) and a Start Time (click the clock icon to choose a specific time in fifteen minute increments), and choose a Time Zone.

Note: Network provisioning tasks (or any operation that queries for or changes device configurations through Grid Manager, including Discovery) are subject to a feature called Blackout periods, which are defined elsewhere in Grid Manager. Blackouts are a scheduled feature that instructs Grid Manager not to perform Discovery operations and Port Control/provisioning operations on the managed network at specified times, days and dates. See the section Defining Blackout Periods for details.

Scheduling Additions and Modifications

You can schedule the addition and modification of an object. For example, you can schedule the addition of a DNS forward zone or the modification of a fixed address. After you schedule a task, administrators cannot modify the object associated with the scheduled task until after the appliance executes the task. However, the object can still be updated with DHCP leases and other system services.
To schedule an addition or a modification:

1. Add or modify a record following the instructions described in this guide.
2. Click the Schedule icon at the top of the corresponding wizard or editor.
3. In the Schedule Change panel, complete the following:
Scheduling Appliance Operations

The appliance supports the scheduling of the following operations:

- **IP discoveries**—For information, see *IP Discovery and vDiscovery.*
- **Service restarts**—For information, see *Restarting Services.*

Scheduling Deletions

You can schedule the deletion of an object or an operation for a later date and time. However, you cannot schedule the deletion of a previously scheduled task.

To schedule a deletion:

1. Navigate to the object.
2. Select **Schedule Deletion** from the Delete drop-down menu.
3. In the **Schedule Deletion** dialog box, complete the following:
   - **Delete Now:** Select this to delete the object upon clicking **Delete Now.**
   - **Delete Later:** Select this to schedule the deletion at a later date and time. Complete the following:
     - **Date:** Enter the date in YYYY-MM-DD (year-month-day) format. The appliance displays today's date. You can also click the calendar icon to select a date from the calendar widget.
     - **Time:** Enter the time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.
     - **Time Zone:** Select a time zone for the scheduled date and time from the drop-down list. This field displays the time zone of the browser that the admin uses to log in to Grid Manager.

4. Click **Schedule Deletion.**

The appliance performs the deletion at the scheduled date and time.

Scheduling Recursive Deletions of Network Containers and Zones

Superusers can determine which group of users are allowed to schedule the deletion of a network container and its child objects as well as a zone and its child objects. For information about how to configure the recursive deletion of network containers and zones, see *Configuring Recursive Deletions of Networks and Zones.*

To schedule the recursive deletion of network containers and zones:

1. Navigate to the object.
2. Select **Schedule Deletion** from the Delete drop-down menu.
3. In the **Schedule Deletion** dialog box, complete the following:
   - **Delete Now:** Select this to delete the object upon clicking **Delete Now.**
   - **Delete Later:** Select this to schedule the deletion at a later date and time. Complete the following:
     - **Date:** Enter the date in YYYY-MM-DD (year-month-day) format. The appliance displays today's date. You can also click the calendar icon to select a date from the calendar widget.
     - **Time:** Enter the time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.
     - **Time Zone:** Select a time zone for the scheduled date and time from the drop-down list. This field displays the time zone of the browser that the admin uses to log in to Grid Manager.

4. Select one of the following:
   - **Delete only the parent container:** Select this to delete only the parent objects and re-parent the child objects.
   - **Delete the parent container and its children:** Select this to delete the parent objects and all its child objects.

4. Click **Schedule Deletion.**

The appliance performs the deletion at the scheduled date and time.

Viewing Scheduled Tasks

After you schedule a task, you can view the pending task in the **Administration tab -> Workflow tab -> Task Manager** tab. For more information, see *Viewing Tasks.* Superusers can view all scheduled tasks, and
limited-access admins can view their own scheduled tasks. In certain panels such as the Network list panel and Smart Folders, Grid Manager displays a calendar icon next to objects that are associated with scheduled tasks, except for the addition of an object. You can click the icon to view the configuration and schedule. You can also reschedule the task if you are the owner of the task, a superuser, or an approver of the task (after you have approved it). In the corresponding editor, the Schedule icon is green when there is a pending scheduled task. For information, see Icons for Scheduled Tasks.

Icons for Scheduled Tasks

Grid Manager displays a scheduled task icon next to an object that is associated with a scheduled task (except for the addition of an object), as shown in Figure 1.11. When you mouse over the icon, an informational dialog box appears displaying the type of action, the date and time of the scheduled task, and the person who scheduled the task. You can click the icon and Grid Manager displays the corresponding editor (for modification) or the Scheduled Deletion dialog box (for deletion) in the read-only mode. If you are viewing a task that you scheduled, you can modify and save the schedule, but you cannot modify the configuration of the object. If you are not the owner of a scheduled modification or a superuser, you can only view the information. You cannot reschedule the task. If you are not the owner of a scheduled deletion or a superuser, Grid Manager does not display the Scheduled Deletion dialog box when you click the icon.

Figure 1.11 Icon for a Scheduled Task

![Icon for a Scheduled Task]

Grid Manager displays a scheduled task icon next to an object that is associated with a scheduled task, as shown in Figure 1.12. You can click the Schedule icon to view the date and time of the scheduled task. You can also reschedule the task if you have the applicable permissions. For information, see Rescheduling Tasks.

Figure 1.12 Scheduling Icon Indicating a Pending Task

![Scheduling Icon Indicating a Pending Task]

Pending Tasks for Operations

You can view all pending tasks for a network discovery or service restart in Task Manager if you have the applicable permissions. For information, see Viewing Tasks. You can also view the pending tasks in their corresponding dialogs.

To view the pending tasks in an editor:

1. Network Discovery: From the Data Management tab, select the IPAM tab, and then click Discovery from the Toolbar.

Service Reboots for the Grid: From the Data Management tab, select the IPAM, DHCP or DNS tab, and then click Restart Services from the Toolbar.

Service Reboots for Grid members: From the Data Management tab, select the DHCP or DNS tab -> Members tab, select a member check box, and then click Restart Services from the Toolbar.

2. Click the Schedule icon at the top of the wizard, and then select Click here to view/manage the scheduled items. Note that this link appears only when you have one or more scheduled tasks.

3. Grid Manager displays the following information in the Scheduled Tasks:

   - Scheduled Time: The date, time, and time zone when the appliance executes the task.
   - Submitted Time: The date, time, and time zone when the task was submitted.
Submitter: The admin who scheduled the task.
TaskDetails: The message that appears in the audit log.

By default, the appliance sorts the tasks by Scheduled Time starting with the earliest scheduled start time. You can do the following in this viewer:

- Sort the tasks in ascending or descending order by column, except for Task Details.
- Reschedule a selected task. For information, see Rescheduling Tasks Associated with Operations.
- Delete a selected task by selecting the task check box and clicking the Delete icon.
- Export and print the information in the table.

Rescheduling Tasks

Superusers can reschedule any scheduled task. Limited-access admins can reschedule only the tasks that they scheduled, depending on their permissions. Approvers can reschedule tasks that they have approved, if they have the scheduling permission. You can reschedule a task from different panels of Grid Manager, depending on your permissions. When you reschedule a task from the object list panel, Grid Manager displays the object or operation configuration in a read-only mode. You can modify the date and time to reschedule the task. However, you cannot modify the configuration of the object or operation. You can also reschedule your own task or a task you have approved from Task Manager.

To reschedule tasks associated with objects, see Rescheduling Tasks Associated With Objects.
To reschedule tasks associated with operations, see Rescheduling Tasks Associated with Operations.

Rescheduling Tasks Associated With Objects

You can reschedule a task associated with an object from the Scheduled Tasks viewer or in an editor if you have the applicable permissions.

To reschedule a task from Task Manager:

1. From the Administration tab, select the Workflow tab -> Task Manager tab -> scheduled_task check box, and then click the Reschedule icon.
2. In the Reschedule dialog box, modify the date and time when you want the appliance to execute the task. You can select Now to execute the task when you save the entry.
3. Save the configuration and click Restart if it appears at the top of the screen.

To reschedule a task in an editor:

1. Navigate to the object with a scheduled task that you want to reschedule.
2. Click the scheduled task icon next to the object.
3. For modification: In the editor, click the Schedule icon at the top of the editor. In the Schedule Change panel, modify the date, time, and time zone. You can also select Now to execute the task upon saving the entry.
   - For deletion: In the ScheduleDeletion dialog box, modify the date, time, and time zone. You can also select Delete Now to delete the object upon clicking Delete Now. The appliance puts the deleted object in the Recycle Bin, if enabled.
4. Save the configuration and click Restart if it appears at the top of the screen.

Rescheduling object change tasks and associated port control tasks is a special case allowing for rescheduling of both tasks in the same editor:

Figure 1.13 Rescheduling an object change task and a port control task
Rescheduling Tasks Associated with Operations

To reschedule a network discovery or a service restart:

1. From the Administration tab, select the Workflow tab -> Task Manager tab -> scheduled_task check box, and then click the Reschedule icon.
   
   or
   
   Navigate to the operation and click the Schedule icon at the top of the wizard. In the Schedule Change panel, select Click here to view/manage the scheduled items. Grid Manager displays all scheduled tasks related to the operation in the Scheduled Tasks viewer. Select the task check box, and then click the Reschedule icon.

2. Grid Manager displays detailed information about the task in the Reschedule dialog box.

3. Modify the date and time when you want the appliance to execute the task. You can also select Now to execute the task when you save the entry.

4. Save the configuration and click Restart if it appears at the top of the screen.

Canceling Scheduled Tasks

To cancel a scheduled task:

1. From the Administration tab, select the Workflow tab -> Task Manager tab -> scheduled_task check box, and then click the Delete icon.

2. In the Confirm Delete Request dialog box, click Yes.

The appliance deletes the scheduled task and does not perform the scheduled operation. Therefore, no change is made to any record after you delete a scheduled task.

Configuring Approval Workflows

Approval workflows support routing certain core network service tasks submitted by an admin group to another for approval. You can add an admin group to an approval workflow and define the group as a submitter or approver group. Note that only superusers can create approval workflows. For information about how to set up admin groups, see About Admin Groups.

In an approval workflow, you can add a submitter group and an approver admin group that you have previously defined. You can also define when and to whom email notifications are sent, and configure options such as whether submitters or approvers must enter a comment or a ticket number when they submit tasks for approval. Approval workflows are useful when you want to control tasks that require reviews. For example, if you have a group of help desk users who can add, modify, and delete hosts and you want members of an operation group to review these tasks, you can define the help desk users as submitters, and then set up members of the operation group as approvers. You can then add the submitter and approver groups to an approval workflow and configure notifications options and other configurations, such as allowing the approvers to reschedule the submitted tasks.

Not all core network service tasks can be routed for approval. You can configure approval tasks associated with certain objects. For a list of supported objects, see Supported Objects for Scheduled and Approval Tasks.

**Note:** When an admin group is defined as a submitter group, there are certain operations the submitters cannot perform even though they may have the permissions to do so. For information about such operations, see 4820042

To create an approval workflow, complete the following:
1. If you have not already done so, set up admin groups that you can configure as submitter groups and approver groups in an approval workflow, as described in About Admin Groups.

2. Create an approval workflow and configure email notifications and other options, as described in 4820042.

You can do the following after you have created approval workflows:

- View a list of approval workflows, as described in 4820042.
- Modify approval workflows, as described in 4820042.
- Delete approval workflows, as described in 4820042.
- View a list of approval tasks, as described in 4820042.
- View approval notifications, as described in 4820042.

### Supported Tasks for Different Admin Groups

Depending on your admin permissions, you may or may not be able to perform certain tasks that are subject to approvals. 4820042 lists specific tasks and indicates which admin group can perform the tasks.

Table 1.2 Supported Tasks for Admin Groups

<table>
<thead>
<tr>
<th>Admin groups that can perform the task</th>
<th>Submitters</th>
<th>Approvers</th>
<th>Superusers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the schedule of a task when it is pending approval</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Change the schedule of a task after it has been approved</td>
<td>Yes (Task is re-submitted for approval)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Execute the task now when it is pending approval</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Delete a task after it has been approved but pending execution</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Delete a task after it failed or has been executed</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Delete tasks by selecting the Select all objects in this dataset option</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note: Not all tasks are deleted, depending on the task status and the admin who performs the deletion

Creating Approval Workflows

Before you create an approval workflow, ensure that you have admin groups that you can define as submitter groups and approver groups. Note that a submitter group can be added to only one approval workflow, and approver groups can be added to multiple workflows. An approver can choose to approve a task and either keep or change the date and time when the task is executed. For information about scheduling and rescheduling tasks, see Scheduling Tasks. An approver can also reject a submitted task.

All submitted tasks are executed based on submitter permissions. When an admin submits a task, the appliance logs the task in the audit log and associates it with a task ID. You can view your tasks in Task Manager, as described in Viewing Tasks. Depending on your configuration, you can control when and to whom email notifications are sent. For example, you can configure the appliance to send notifications to only the approver each time when a task requires approval, or send notifications to both the submitter and approver group each time when a task is disapproved.

To create an approval workflow:

1. From the Administration tab, select the Workflow tab -> Approval Workflows tab, and then click the Add icon.

2. In the Add Approval Workflow wizard, complete the following:

   - **Submitter Group**: From the drop-down list, select the admin group whose submitted tasks require approvals. Note that performing CSV imports do not require approvals. If there is a warning that the submitter group has CSV import permission, you may want to remove the permission.

   - **Approver Group**: From the drop-down list, select the group that can approve tasks submitted by admins of the submitter group. If the approver group you select does not have the permission to schedule tasks, the approvers cannot reschedule the execution dates and times of the tasks when they approve them.

   - **Ticket Number**: From the drop-down list, select one of the following to determine whether a ticket number is required when a submitter submits a task for approval:
     - **Required**: The submitter must enter a ticket number when submitting a task.
     - **Optional**: The submitter can choose to enter a ticket number or not when submitting a task.
     - **Not Used**: The Ticket Number field does not appear when the submitter creates a task.

   - **Submitter Comment**: From the drop-down list, select whether the submitter must enter a comment or not when submitting a task for approval. You can select Required, Optional, or Not Used.

   - **Approver Comment**: From the drop-down list, select whether the approver must enter a comment or not when approving a task. You
can select Required, Optional, or Not Used.

3. Click Next and complete the following to specify notification options for the workflow:

- **Approver Notification Address(es):** Select one of the following to specify to which approver email addresses the appliance sends workflow notifications. The default is **Group Email Address(es).**
  - **Group Email Address(es):** Select this if you want the appliance to send notifications to the list of email addresses configured for the admin group. For information about how to configure this list, see About Admin Groups.
  - **User Email Address(es):** Select this if you want the appliance to send notifications to individual email addresses of the admin group.
- **Notifications sent on:** Select the operations that can trigger email notifications. When you select an operation, the appliance sends a notification each time that operation occurs. By default, all operations are selected.
  - **Approval Required:** The appliance sends an email notification each time an approval is required.
  - **Task Approved:** The appliance sends an email notification each time a task is approved.
  - **Task Rejected:** The appliance sends an email notification each time a task is rejected.
  - **Task Succeeded:** The appliance sends an email notification each time a task is completed successfully.
  - **Task Failed:** The appliance sends an email notification each time the execution of a task fails.
  - **Task Rescheduled:** The appliance sends an email notification each time a task is being rescheduled.
- **Notifications sent to:** For each operation, select whether the Approver, Submitter, or Both are notified when the operation occurs. The default value is Both for all operations. For information about email notifications, see 4820042

4. Optionally, click Next to add extensible attributes to the approval workflow. For information, see About Extensible Attributes.
5. Save the configuration.

### Viewing Approval Workflows

Grid Manager lists all approval workflows in the Approval Workflows tab. Only superusers can view approval workflows defined for the Grid. Limited-access users cannot view approval workflows.

To view approval workflows:

1. From the Administration tab, select the Workflow tab -> Approval Workflows tab.
2. Grid Manager displays the following for each approval workflow:
   - **Submitter Group:** The name of the admin group whose tasks require approvals.
   - **Approver Group:** The name of the admin group that can approve tasks submitted by members of the submitter group.
   - **Ticket Number:** Displays whether the submitter is required to enter a ticket number when submitting tasks that require approvals. Possible values are Not Used, Optional, and Required.
   - **Submitter Comment:** Displays whether the submitter is required to enter a comment when submitting tasks that require approvals. Possible values are Not Used, Optional, and Required.
   - **Approver Comment:** Displays whether the approver is required to enter a comment when approving tasks. Possible values are Not Used, Optional, and Required.
   - **Site:** Values that were entered for this predefined extensible attribute.

You can do the following in this tab:

- Modify some of the data in the table. Double click a row, and either modify the data in the field or select an item from a drop-down list. Click Save to save the changes. Note that some fields are read-only.
- Sort the data in ascending or descending order by column.
- Select an approval workflow and click the Edit icon to modify data, or click the Delete icon to delete it.
- Use filters and the GoTo function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Print and export the data in this tab.

### Modifying Approval Workflows

You can modify information in an approval workflow, except for the submitter group. To modify approval workflow configuration:

1. From the Administration tab, select the Workflow tab -> Approval Workflows tab.
2. Select an approval workflow and click the Edit icon.
3. Grid Manager provides the following tabs from which you can modify information:
   - **General** tab: You can modify the approver group and decide whether the ticket number, submitter comment, and approver comment are required, but you cannot change the submitter group. For information, see 4820042.
   - **Approval Notifications** tab: You can modify when and to whom email notifications are sent. For information, see 4820042.
   - **Extensible Attributes** tab: You can add or modify values of extensible attributes. For information, see About Extensible Attributes.
4. Save the configuration.
Deleting Approval Workflows

You can delete an approval workflow any time after you have created it. Note that when you delete a workflow that has associated tasks that are pending approvals, the tasks will be rejected after you delete the workflow.

To delete an approval workflow:

1. From the Administration tab, select the Workflow tab -> Approval Workflows tab.
2. Select an approval workflow and click the Delete icon.
3. Click Yes in the Delete Confirmation dialog.

Viewing Approval Tasks

If you belong to an approver admin group, you can view, approve, or reject tasks that are pending your approval in the Task Manager tab. For information, see Viewing Tasks. Submitters can view all pending and completed tasks they have submitted.

Viewing Workflow Notifications

When a submitter and approver receives an email notification about their tasks, the appliance lists the approval status and workflow related information such as task ID, submitter name, execution time, object type and action in the email notification.

Following is a sample email notification:

Notification:
--------------
Message: Task 32 submitted by subm has been approved The following task has been approved: Task details

Click here to go to the task management tab - https://192.168.1.2/ui/?contextId=taskmanager

Note: When you can click the hyperlink displayed in the notification, you can log in to Grid Manager and access the Task Manager tab in a separate browser tab or window.

Unsupported Operations for Submitters

When admins are part of a submitter group in an approval workflow, there are certain operations they cannot perform even though they may have the permissions to do so. Following is the list of operations that submitters cannot perform:

- Reclaim IPv4 or IPv6 addresses
- Expand networks
- Resize networks
- Split networks
- Sign (DNSSEC) zones
- Unsign DNSSEC signed zones
- Import DS to DNSSEC signed zones
- Perform KSK rollovers on a DNSSEC signed zones
- Copy records from one DNS zone to another
- Clear all discovered data
- Clear discovered timestamps
- Clear unmanaged addresses
- Resolve discovery conflicts
- Update extensible attributes on multiple objects at the same time
- Delete or modify several objects at a time (using the "Select all objects in this dataset" option from Grid Manager)
- Order DHCP Ranges inside a network (feature is available only when used with Sophos)
- Configure member DHCP Captive Portal through the wizard
- Restore objects from the Recycle Bin
- Delete non-native NIOS DNS resource records. These objects can only be synchronized from a Microsoft DNS server
- Copy rules from one Response Policy Zone to another
- Order Response Policy Zones
About Long Running Tasks

A long running task is a task that requires more than 30 seconds to complete and involves a large amount of data. When Grid Manager performs a long running task, it displays the Long Running Task dialog box that indicates whether you can run the task in the background. You can navigate to another tab or perform other functions only if the task can be run in the background. For information, see 481721.

Grid Manager disconnects if a task takes more than five hours to perform. Though you can log back in to Grid Manager while the appliance continues to perform the task, Grid Manager does not display the progress of the task.

Note: You cannot stop a long running task once you start it.

The appliance supports the following long running tasks:

- Restoring the database
- Backing up the database
- Backing up licenses
- Signing DNS zones
- Unsigning DNS zones
- Exporting DS records and trust anchors
- Deleting all objects in a table or dataset
- Modifying multiple extensible attributes
- Viewing DNS and DHCP configuration properties
- Migrating bloxTools data
- IPAM tasks on the Tasks Dashboard
- Downloading the following:
  - Audit logs
  - Syslog files
  - Support bundles
  - SNMP MIB files
  - NTP keys
  - HTTPS certificates
  - Traffic capture

Running Tasks in the Background

Grid Manager allows certain long running tasks to run in the background. You can navigate to other tabs and perform other functions when Grid Manager performs tasks in the background. However, when you make changes to objects that are currently affected by a long running background task, Grid Manager does not save the changes until after the long running task is completed. Grid Manager can perform up to 10 background tasks at a time.

You can run the following tasks in the background:

- Signing DNS zones
- Unsigning DNS zones
- Modifying multiple extensible attributes
- Deleting all objects in a table or dataset
- Migrating bloxTools data

To run a task in the background:

1. Perform the task following the instructions described in this guide.
2. In the Long Running Task dialog box, click Run in Background.

You can view the progress of the task by clicking the progress bar at the top of the interface. For information, see 4817221.

Monitoring Long Running Tasks

When you have one or more tasks running in the background, Grid Manager displays a progress bar next to the Global Search icon at the top of the interface. You can click the progress bar to view detailed information about the tasks in the Background / Long Running Task viewer. In this viewer, Grid Manager displays a progress bar for each task that is currently running in the background. When all background tasks are completed, the progress bar at the top of the interface disappears. Grid Manager displays a message at the top of the interface when the task is completed successfully or if the task fails.

For other tasks that you cannot run in the background, the Long Running Task dialog box remains open until the task is completed. You cannot navigate to other tabs or perform other functions when the long running task is in progress. Grid Manager closes the dialog box when the task is completed. It also displays a message at the top of the interface when the task is completed successfully or if the task fails.

About CSV Import

Use CSV Import to import DNS, DHCP, and IPAM data through Grid Manager. You can use this feature to migrate or add new data, overwrite existing data, merge new data with existing data, delete existing data, or replace certain existing data in the database.
To import new data, you must first prepare a data file (include all required fields and follow the proper syntax), and then start an import through Grid Manager. You can also export existing data to a data file, modify the data, and then import the modified data to the database. You can either overwrite existing data with the modified data or merge new data with the existing data. You can also delete data that is no longer required or replace certain existing data with new data in the file. Note that the replace option is valid for authoritative zone data only whereas other options are valid for all supported objects including zones. The replace operation creates a snapshot or a backup of the existing data in the database before replacing the database with the data in the imported CSV file.

The appliance supports CSV import for most record types. You can use IDNs and punycode for the domain name field for most of the DNS object types. For information about IDNs and punycode, see Support for Internationalized Domain Names. Only superusers can import A and AAAA records with a blank name. Limited-access users must have read/write permission to Adding a blank A/AAAA record in order to import A and AAAA records with a blank name, otherwise the CSV import operation might fail. You can assign global permission for specific admin groups and roles to allow to import A and AAAA records with a blank name. For more information, see Administrative Permissions for Adding Blank A or AAA A Records. For each supported record type, you must include all required fields in the header row of the dataset that you want to import. For a list of supported record types and specific guidelines for creating a data file, refer to the Infoblox CSV Import Reference.

To import a data file:

1. Create a data file if you do not already have one. Follow the guidelines for the supported objects to ensure that you include all the required fields in the file. For more information, refer to the Infoblox CSV Import Reference. You can also export existing data and then update the file for re-import. For information, see 3247403 3247403 3247403.
2. Start a CSV import. For information, see Exporting Displayed Data.

**WARNING:** CSV imports and operations that involve massive data, such as deleting large zones and recursive deletion of networks and all child objects, will significantly affect member performance, resulting in service outage.

When you submit multiple CSV imports, the appliance puts the import jobs in queue and executes them one at a time in the order they are submitted. When a job is being executed, it is in the Import in progress state. When a job is in queue for execution, it is in the Import pending state. You can import multiple CSV files at a time, but at any given time you can execute only one single task. Note that only one task at a time will be in the Import in progress state, while the others are in the Import pending state. You can view the status of each import job through CSV Job Manager. Superusers can view all import jobs while limited-access users can view only the jobs they submitted.

To access CSV Job Manager, from the Data Management tab, click CSV Job Manager from the Toolbar and select Jobs Manager, or from the Tasks Dashboard, click CSV Import in the IPAM Task Pack. Superusers and limited-access users that have applicable configurations and permissions can perform CSV imports and exports. For information about user permissions for CSV imports and exports, see 3247403. You can do the following in CSV Import:

- Add, overwrite, append, replace or delete data through the imported CSV file, as described in 3247403 3247403 3247403.
- Verify the content in the CSV file, as described in 3247403.
- View a list of CSV import jobs, as described in 3247403 3247403.
- Add and start CSV import jobs, upload data files, stop CSV imports, or edit the options of the uploaded file, as described in 3247403.
- Delete uploaded jobs, as described in 3247403.
- Download the following: imported files, import errors, import results, or snapshots, as described in 3247403.
- Select a pending or saved job, and then click the Cancel icon to cancel the job.
- Click the Refresh icon to refresh the CSV Job Manager.

Note that superusers can view any jobs in the CSV Job Manager, and limited-access users can only view jobs they submitted.

**Note:** The list of CSV import jobs are not restored when you restore a backup file or when you promote a master candidate.

### CSV Import User Permissions

Superusers can perform any CSV import tasks. You must assign limited-access users the correct configurations and permissions so they can perform CSV imports and exports. For information about how to configure the CSV Import task for limited-access users, see About Dashboard Templates. Limited-access users can import data to which they have proper permissions. For information about admin permissions, see About Administrative Permissions.

Changes you make to user permissions can affect CSV import and export behaviors. The following table lists actions performed on user permissions and the corresponding effects on CSV imports and exports:

<table>
<thead>
<tr>
<th>Actions taken on user permissions</th>
<th>CSV import and export behaviors associated with the affected user account</th>
</tr>
</thead>
</table>
| Delete a user account            | - CSV import jobs remain in the system and are accessible by superusers only.  
                                  | - All pending import jobs cannot be executed due to authentication failures.  
                                  | - If the action is taken during an import job that is in progress, the rest of the import will fail.  
                                  | - All stopped and successful jobs are available to superusers only. |

Copyright ©2019, Infoblox, Inc. All right reserved.
CSV Import Limitations

Ensure that you understand the following limitations before you start an import:

- You can import multiple CSV files at a time, but at any given time you can execute only one single task. The import tasks are queued. Note that only one task at a time will be in the Import in progress state, while the others are in the Import pending state.
- Do not use UTF-8 characters in the CSV file name.
- When you perform a CSV import that includes objects that have scheduled changes or updates associated with them, the import fails. Only superusers can cancel the scheduled changes.
- When you stop an import, the appliance completes the import of the data row it is currently processing before it stops the import. You cannot resume the import from where it stopped.
- You cannot roll back to previous data.
- The following data cannot be imported: Microsoft management, DNSSEC, and GSS-TSIG data.
- CSV import does not support DNSSEC zones, though resource records added for a signed zone are supported.
- Only editable data can be imported or manipulated.
- When you promote a new Grid Master during an import, the import stops; and it does not restart on the new Grid Master. When a failover occurs during an import, the import stops on the old active node, and it does not restart on the new active node.
- It may take longer than expected to import a large number of DHCP ranges that are associated with a single MAC address filter.
- When a CSV import starts, the appliance validates the first 100,000 rows of data in the CSV file. If the file contains more than 100,000 rows of data, the appliance validates the rest of the data as the import progresses.
- The appliance supports up to one million rows of data in each CSV import.
- You cannot import network containers.
- To successfully import RIR (Regional Internet Registries) organizations, you must also specify the maintainer password. Note that the password field is not exported during a CSV export. For information about RIR updates, see RIR Registration Updates.
- You can use the Replace operation to replace the current data in the database with the data in the imported CSV file. Note that the replace option is valid for authoritative zone data only whereas the other options are valid for all supported objects including zones. For more information, see 3247403.
- The Replace operation is available only for authoritative zones. This operation does not support DNS records that are automatically generated or exported, but it supports NS records that are created manually.
- Use the delete function to delete import jobs that are uploaded. You can delete the content of a CSV file that you have imported to the database. Note that you cannot delete jobs that are already imported.
- When you import CSV files for NS record updates, you must specify a value for zone_nameservers. NIOS displays an error message if you do not specify a value for this field when you import the CSV file.
- When you perform a CSV export of automatically created NS records using Infoblox API, the zone_nameservers field will have an empty value. Therefore, if you import the previously exported CSV file that includes automatically created NS records through the Infoblox GUI, then the CSV import fails and Grid Manager displays an error message.
- If you upload a file and preview the file using the Preview option, and later update the content of the same CSV file, and then try to view the edited file using the same Preview wizard, you may not be able to see the changes. Infoblox recommends that you start a fresh CSV import to upload the edited file and navigate to the Preview wizard to preview the file.
- You cannot perform the CSV import operation on a Microsoft Server zone object, but NIOS allows you to perform the CSV import operation on records within a Microsoft Server zone. You may not see an error message when you perform a CSV import using the replace operation on an Microsoft Server zone.

Configuring Import Options

You can import CSV files and perform various operations to update the data in the database. You can choose from several import options: add, override, merge, delete, and replace. You can add new rows from the imported file to the database, overwrite existing rows in the database, append rows to the existing rows in the database, delete existing rows in the database, or replace the existing rows in the database. You can verify whether the data in the imported file is appropriate using the Test option before you import the file to the database. You can also view the results and progress details of the operation.

To import a CSV file, complete the following:

1. From the Data Management tab, click CSV Job Manager from the Toolbar.
2. In the CSV Job Manager wizard, select CSV Import and click the New CSV import job icon.
3. In the New CSV Import Wizard, complete the following:

Type of Import

For all supported objects (including zones)

- **Add**: Select this to add new rows from the imported CSV file to the database. NIOS updates the database with the new data that you have added to the imported CSV file and retains the rows that do not have any changes.
- **Override**: Select this to overwrite the existing data in the database with the data from the uploaded file. You cannot add new rows or delete existing rows. If you want to overwrite values in the required fields, you must include the required fields and the corresponding
For zones only

- **Replace**: Select this to replace the contents of the database with data provided in the CSV file. NIOS cancels the replace operation and will not save the changes if it encounters an error. You can replace the DNS records of a zone by importing a zone file that was exported previously. You can only replace DNS records that are manually created. NIOS generates a results file listing the file name, action performed, date and time, and result at the end of the validation. You can view the results file only after the replace operation is complete. NIOS generates the backup file automatically for every replace operation and saves it in the Infoblox Grid. Note that the CSV file must contain data for one authoritative zone only, that is, you cannot insert records from different authoritative zones into a single CSV file for replace operation.

**Note**: The replace operation might affect system performance if you try to replace a zone with a lot of changes. Infoblox recommends that you perform the replace operation for large import files (more than 10,000 rows of changes) during non-peak hours. This operation ignores _new_XXX fields in the imported CSV files.

4. Click **Next** to import the CSV file.
   - **Import Type**: Displays the type of import option you have selected.
   - **Select the CSV file that you want to import and click Choose**.
   - **On Error**: Select one of the following to tell the appliance what to do when it encounters an error during an import:
     - **Stop import**: Select this to stop the data import once it encounters an error in the uploaded file. Grid Manager displays the row number at which it stops the import when it encounters an error. NIOS saves the changes made to the CSV file before an error occurs. For example, if there are 100 rows of data and you select this option, and there is an error in row 90, the appliance displays **90 of 100 completed, 1 error**.
     - **Skip to the next row and continue**: Select this to skip over errors and continue the data import. You can download an error report to identify the erroneous data. NIOS displays the total number of rows it has processed by skipping over. For example, if there are 100 rows of data and you select this option, the appliance displays **100 of 100 completed, 1 error**.

5. Click **Next** to preview your CSV file. In the File Preview table, Grid Manager displays the header row, the first six rows, and up to 15 columns of the imported data. You cannot edit the data here. Field names with asterisks ⭐ indicate required fields. Note that you must define these fields in the imported file. If any of the required fields are missing, the appliance generates an error during the import operation. You can do the following in this wizard:
   - **Import type**: The type of import option you have selected.
   - **Filename**: The name of the CSV file you have selected.
   - **Separator**: Select a separator for your CSV file from the drop-down list. The default value is **Comma**.
   - **OnError**: The option you have selected.

6. Click **Test** to verify the content in your CSV file. Click **Yes** in the TestCSVImportForReplaceOperation dialog box to verify the content or click **No** to cancel the operation. NIOS automatically analyzes the data in the imported file for any syntax errors or other violations. You can also view a detailed report of the file that you are importing. Note that you can run the test as a background task. This report also displays information about the number of deleted, updated and added files. It also displays error messages, if any. NIOS generates a results file listing the file name, action performed, date and time, result, and the number of failures at the end of the validation. You can view the results file only after the replace operation is complete.

**Note**: The **Test** button is enabled only when you select the **Replace** operation and is disabled for other import options.

7. Click **Import** to import the CSV file to the database. Click **Yes** in the dialog box to import the CSV file or **No** to cancel the operation.

8. You can view the progress and results of your import operation in the **CSV Import Progress** wizard. This wizard displays the following information:
   - **Import type**: The type of import option you have selected.
   - **Filename**: The name of the CSV file you have selected.
   - **Separator**: The separator you have selected for your CSV file. The default value is **Comma**.
   - **OnError**: The option you have selected when the import operation encounters an error.
   - **Current status**: If an import is in progress, this field displays its current status. Otherwise, it displays the date and time of the last import.
   - **Last action**: Displays the last operation and the admin who initiated it.
   - **Rows Completed**: The number of rows of data the import has processed. Depending on the import options, Grid Manager displays either the row number at which it stops an import when it encounters an error or the total number of rows it has processed by skipping over the erroneous data. For example, if there are 100 rows of data and you select "On error: Stop importing," and there is an error in row 90, Grid
Manager displays **90 of 100** here. If you select "On error: Skip to the next row and continue," Grid Manager displays **100 of 100** here and displays **1 in Rows with Errors**.

- **Rows with Errors**: The number of rows of data the import has detected errors. Click **Download Errors** to download the CSV file that contains the fields and the rows of erroneous data. You can use this report as a reference to update the data file before you import the file again.

To cancel the import operation, click **Stop Import** before the operation is complete. To close the wizard and execute the operation in the background, click **Close & Run in Background**. When the operation is complete, you can click **Download** to download and view the errors. The **Download errors** button is enabled only if the operation encounters errors. Click **Save & Close** to save the operation and close the wizard.

**Note**: Superusers can view all CSV import jobs and limited-access users can view only the jobs they submitted.

---

**Viewing CSV Import Jobs**

You can view the status of import jobs. To view the status:

1. From the **Data Management** tab, click **CSV Job Manager** from the Toolbar.
2. In the **CSV Job Manager** wizard, click **CSV Import**. Grid Manager displays the following information about the import jobs that were submitted in the past 30 days:
   - **User Name**: The admin user who submitted the CSV import. Only superusers can view this column.
   - **Status**: The current status of the import job. The status can be one of the following:
     - **Import successful**: The import is completed without errors. Check the **Message** field for information about the import.
     - **Import unsuccessful**: The import is completed, but with errors. Check the **Message** field for information about the error message.
     - **Import pending**: The job is in queue for execution.
     - **Import in progress**: The job is being executed.
     - **Import stopped**: The job has been stopped. You can select the job and restart the import.
     - **Test successful**: Test is completed without errors. Check the **Message** field for information about the test.
     - **Test unsuccessful**: Test is completed, but with errors. Check the **Message** field for information about the error message.
     - **Test pending**: Test is in queue for execution.
     - **Test in progress**: Test is in progress.
     - **Test stopped**: Test has been stopped. You can select the job and restart the import.
     - **Saved file**: The data file has been uploaded, but the import has not started.

**Note**: After a product restart, which can be caused by a failover, all **Import in progress** jobs go into **Import stopped** state; all **Import pending** jobs continue to be queued for execution.

- **Submitted**: The timestamp when the job was submitted.
- **Completed**: The timestamp when the job was completed. This field is blank if the job has not been completed yet.
- **File Name**: The CSV data file name.
- **Message**: This field displays the number of rows of data that have been processed and the number of rows of data the import has detected errors. Depending on the import options, Grid Manager displays the row number at which it stops the import when it encounters an error, or the total number of rows it has processed by skipping over the erroneous data. For example, if there are 100 rows of data and you select "On error: Stop importing," and there is an error in row 90, the appliance displays **90 of 100 completed, 1 error**. If you select "On error: Skip to the next row and continue," the appliance displays **100 of 100 completed, 1 error**.
- **FileSize**: The size of the imported CSV file.

**Note**: Superusers can view all CSV import jobs and limited-access users can view only the jobs they submitted.

---

**Modifying CSV Import Jobs**

You can modify the options of the CSV file that you have already uploaded, delete the jobs that are uploaded, or download uploaded file or error file. After you configure the import options, you can select a data file and start an import operation or upload a data file. For more information about configuring import options, see 3247403 3247403.

To edit the options of a file, complete the following:

- From the **Data Management** tab, click **CSV Job Manager** from the Toolbar.
- In the **CSV Job Manager** wizard, select **CSV Import** and select the import job that you want to update, click the Action icon and select **Edit**.
- In **Edit-CSV Import Job**, select a type of import and perform the operations mentioned in 3247403 3247403.
- Click **Download** to download the uploaded file, snapshot file, or the results file. For more information, see 3247403.

Copyright ©2019, Infoblox, Inc. All right reserved.
Deleting Uploaded Jobs

You can delete import jobs that are uploaded. You cannot delete jobs that are already imported. You can delete the content of a CSV file that you have imported to the database. Note that the CSV import files and the backed up files are saved for a period of 30 days, but the size limit is set to 1 GB. If these files increase in size, NIOS removes the older files from the Grid. NIOS generates a syslog message if it encounters an error when generating the backup file.

Note: When you delete a parent object from the CSV file, the child objects associated with the parent objects are also deleted.

To delete uploaded jobs, complete the following:

1. From the Data Management tab, click CSV Job Manager from the Toolbar.
2. In the CSV Job Manager wizard, select CSV Import and select the import job that you want to delete, click the Action icon and select Delete or click the Delete pending job icon.
3. Click Yes to delete the uploaded job or No to cancel the operation in the Cancel Import Job wizard.

Downloading Files

You can download various types of files based on the import operation that you have selected. You can download the following files: uploaded, error, results, and snapshot. Superusers can download the original imported file.

Downloading Uploaded or Error Files

You can download CSV files that are already uploaded or download error files to check the errors that the import operation encountered. The download options are valid for all import operations, except replace. To download the file, complete the following:

- From the Data Management tab, click CSV Job Manager from the Toolbar.
- In the CSV Job Manager wizard, select CSV Import and select the import job that you want to download, click the Action icon and select Download.
  - Uploaded File: Select this to download the uploaded CSV import file.
  - Error File: Select this to download the error file. This option is enabled only if the import operation encountered an error.

You can export these files to your local system.

Downloading Uploaded, Snapshot, or Results Files

You can view the uploaded, result, and snapshot files. The snapshot and results files are enabled only for replace operation. To download the file, complete the following:

1. From the Data Management tab, click CSV Job Manager from the Toolbar.
2. In the CSV Job Manager wizard, select CSV Import and select the import job that you want to download, click the Action icon and select Edit.
3. In Edit - CSV Import Job, click the arrow beside the Download option and select one of the following:
   - Uploaded File: Select this to download the uploaded CSV import file. The uploaded report displays the content of the imported file, before it was uploaded, that is before the content of the database is changed.
   - Snapshot File: Select this to download the backup file. NIOS automatically creates a backup of the database before replacing the content of the database with the content in the imported CSV file. This option is enabled only for the replace operation. NIOS generates an error message and saves it in the syslog and the infoblox.log file when the backup file is not generated. You can download the backup file after the replace operation is complete. NIOS saves the backup file and other results file in the Grid for a period of 30 days. The name of the backup file has the following format: csv-snapshot-10-\{view\}-\zone]-\{timestamp\}.csv where 10 is the import ID of the CSV import task, view is the DNS view name, zone is the FQDN of the zone being replaced and timestamp is the timestamp at when the file is generated.
   - Results File: Select this to download the results file. The file displays the content of the database after the content of the file replaced the content of the database. You can view the results file only after the replace operation is complete.

You can export these files to your local system.
Creating a Data File for Import

If you are migrating new data into the database, you must prepare the data file using the correct format and syntax before you can import it successfully. You must include all the required fields and understand the dependencies among some of the fields. For detailed information about the guidelines, supported record types, and interdependencies among fields, refer to the Infoblox CSV Import Reference.

Exporting Data to Files

You can export existing data to a CSV file. The appliance marks all required fields with an asterisk⭐ in the exported file. It also adds a _new_XXXX field to each required field so you can use this field to update data. You cannot stop an export once you start it.

**Note:** Limited-access users can export up to 2,000 rows (2,000 objects) of data. For performance reasons, NIOS has limited the objects to 2,000. Only superusers can export data that exceeds 2,000 rows. For example, consider that you are exporting Infoblox::DNS::Host objects. The NIOS appliance displays an output file with 4,000 lines, because the Host record consists of two lines, one for the Host Record and another for the Host Address; however, the total count of objects will still remain 2,000.

To export all data to a CSV file:

1. From Grid Manager, navigate to the panel that contains the data you want to export. For example, if you want to export data for all DNS zones, select the Data Management tab -> DNS tab -> Zones tab.
2. In the panel, select Export data in Infoblox CSV Import format from the Export drop-down menu.
3. In the Export dialog box, complete the following:
   - **Separator:** Select the separator used in the data file. The default is Comma.
   - **Click Export.**

The appliance exports all the fields of the records that are displayed in this panel based on your filter criteria. You can either open the data file or save it to your computer. The appliance uses a default file name depending on the panel from which you perform the export. For example, when you export the data from the IPAM tab, the default file name is Allnetworks.csv. When you export data from the DNS tab, the default file name is Allzones.csv. The file contains a header row that includes all the fields of the corresponding record type. You can update this data file, and then re-import the data into the database.

You can also export the displayed fields in a panel. For information, see Exporting Displayed Data.

- **Exporting New CSV Jobs**

You can use the Global CSV Export Wizard to export multiple objects at once. You can export multiple object data types to a single CSV file through Grid Manager. Objects that have the least or no dependencies on other objects are placed at the top of the list and the most dependent objects are displayed at the bottom of the list. The export command will not re-execute after a Grid Manager HA failover. For standalone appliances, the Grid Manager sends a single CSV export request that contains both Grid and member CSV headers to export Grid and member properties. Similarly, Grid Manager combines GridDns and MemberDns headers to export DNS properties and GridDhcp and MemberDhcp headers to export DHCP properties. You cannot export the default DNS view if you have not created a custom DNS view. To export the default DNS view, you must either create custom DNS views or use the CSV Global Export option.

Note that when you use the Global CSV Export option to export either all objects, all DNS objects, or all PTR records, the appliance also exports the PTR system generated records from the auto-created zone “0.0.127.in-addr.arpa”. When you use the same file for import operation, the CSV import operation might fail due to the presence of these system generated records. Infoblox recommends that you select the **Skip to next row and continue** option while performing the CSV import operation. When you select this option, CSV import skips these rows with appropriate error messages and then processes other rows in the CSV file.

To export DNS and DHCP data:

1. From the Data Management tab, click CSV Job Manager from the Toolbar.
2. In the CSV Job Manager wizard, click CSV Export. Click the New CSV Export job icon and specify the following in the **Global CSV Export Wizard:**
   - **Separator:** Select a separator from the drop-down list: Comma, Semicolon, Space, and Tab.
   - **All Objects:** The check box is selected by default. When you select this check box, all DHCP, global, and DNS objects are selected by default.
     - **All DHCP Objects:** Select this check box to select all DHCP objects that are listed. To select specific DHCP objects, clear this check box and select respective check boxes next to the DHCP object names.
     - **Global Objects:** Select this check box to select all global objects that are listed. To select specific global objects, clear this check box and select respective check boxes next to the global object names.
     - **All DNS Objects:** Select this check box to select all DNS objects that are listed. To select specific DNS objects, clear this check box and select respective check boxes next to the DNS object names.
3. Click Export Data to start the export process. In the Start/global/CSVExport dialog box, click Yes to confirm or click No to cancel the process.
4. Grid Manager displays the CSV export progress and results in the CSVGlobalExportprogress dialog box. It displays the following information:

- **Separator**: The separator used in the CSV file.
- **Approximate number of objects to be exported**: Indicates the total number of objects to be exported.
- **Number of objects exported**: Indicates the total number of objects that are exported.
- **Current status**: Indicates the current status of the export process.

5. Click **Close** to exit.

### Managing CSV Export Jobs

You can view the list of CSV export operations using the **CSV Job Manager**.

1. From the **Data Management** tab, click **CSV Job Manager** from the Toolbar. In the **CSV Job Manager** wizard, click **CSV Export**.
2. Grid Manager displays the following information:
   - **User Name**: The admin user who submitted the CSV export. Only superusers can view this column.
   - **Status**: The current status of the export job. The CSV export process runs in an asynchronous mode similar to the CSV import. The status can be one of the following:
     - **Export pending**: The job is in queue for execution.
     - **Export running**: The job is being executed.
     - **Export stopped**: The job has been stopped. You can select the job and restart the export.
     - **Export completed**: The export is completed without errors. Check the **Message** field for information about the export.
     - **Export failed**: The export is completed, but with errors. Check the **Message** field for information about the error message.
   - **Submitted**: The timestamp when the job was submitted.
   - **Completed**: The timestamp when the job was completed. This field is blank if the job has not been completed yet.
   - **Failed Description**: The appliance displays the error message in the **Failed Description** column if the CSV export fails. You cannot start a failed CSV export task.
   - **File Size**: The size of the generated CSV file.

Completed CSV export jobs are deleted 30 days from the date of submission. You can also perform the following operations:

- Select a completed CSV export task and download the exported file.
- Cancel or stop a pending CSV export task using the **Delete** option.
- Purge all export tasks after an upgrade or restore.
- Start a new global CSV export job.

### Modifying CSV Export Jobs

You can cancel an export job that is in progress or download an exported job. You can also schedule new export jobs. The appliance deletes the CSV jobs that are completed after 30 days from the date of submission.

To update an exported job or delete one:

1. From the **Data Management** tab, click **CSV Job Manager** from the Toolbar.
2. In the **CSV Job Manager** wizard, click **CSV Export**.
3. Select the export job that you want to update, click the Action icon

   ![Action Icon]

   Click **Cancel** to cancel the export job that is in progress. You can also click the **Cancel job** icon to delete the file. Click **Download file** to download the exported file. For more information, see 3247403.
4. Click the New CSV Export job icon to export a new job. For more information, see 3247403.
5. Click **Close** to exit.

### Exporting Displayed Data

You can export visible information, such as global search results and the syslog file, in CSV format from panels and pages that support the Export function, and then easily convert the file to PDF and other file formats. You can also export all data in a specific panel. For information, see Exporting Data to Files.

To export displayed data:

1. From Grid Manager, navigate to the panel that contains the data you want to export. For example, if you want to export data for DNS zones, select the **Data Management** tab -> **DNS** tab -> **Zones** tab.
2. In the panel, select **Export visible data** from the **Export** drop-down menu.
3. In the **Export** dialog box, click **Start**. Grid Manager displays a message about the time required to export data could be long depending on the amount of data.
4. Click **Download** when the export is finished.
5. Depending on your browser and operating system, you may need to do one of the following in the **Opening .csv** dialog box:
   - **Open with**: Select a program with which you want to open the .csv file.
• **Save to Disk**: Select this if you want to save the .csv file to your local computer.

• **Do this automatically for files like this from now on**: Select this check box if you want Grid Manager to use the same method for future exports. When you select this check box, Grid Manager does not display the Opening .csv dialog box in the future.

6. Click **OK**.

Depending on the selected option, Grid Manager opens the file using the program you select, or saves the file to your local computer.

### Printing from Grid Manager

In Grid Manager, you can print information from panels and pages that support the Print function. Grid Manager prints data one page at a time. The amount of data that is displayed in a specific panel depends on the table size configuration that you set in your user profile. For information, see **Specifying the Table Size**.

To print:

1. Click the **Print** icon. You must allow pop-up windows in your browser for printing. Grid Manager displays a separate browser window.
2. Click **Print**.
   - Grid Manager displays the **Print** dialog box.
3. Configure printer settings and parameters.
4. Depending on your browser, click **OK** or **Print**.

### Multilingual Support

The NIOS appliance supports UTF-8 (Unicode Transformation Format-8) encoding for the following:

- Hostnames for Microsoft Windows clients that support Microsoft Windows code pages. For information, see **Configuring UTF-8 Encoding for Hostnames**.
- Input fields through Grid Manager. For information, see **UTF-8 Supported Fields**.

UTF-8 is a variable-length character encoding standard for Unicode characters. Unicode is a code table that lists the numerous scripts used by all possible characters in all possible languages. It also has a large number of technical symbols and special characters used in publishing. UTF-8 encodes each Unicode character as a variable number of one to four octets (8-bit bytes), where the number of octets depends on the integer value assigned to the Unicode character. For information about UTF-8 encoding, refer to RFC 3629 (UTF-8, a transformation format of ISO 10646) and the ISO/IEC 10646-1:2000 Annex D. For information about Unicode, refer to The Unicode Standard.

Depending on the OS (operating system) your management system uses, you must install the appropriate language files in order to enter information in a specific language. For information about how to install language files, refer to the documentation that comes with your management system.

### UTF-8 Supported Fields

The NIOS appliance supports UTF-8 encoding in all of the comment fields and most input fields. You can enter non-English characters in these data fields through Grid Manager and the Infoblox API. When you use the Infoblox API, all the non-ASCII strings must be UTF-8 encoded so that you can use Unicode characters. The NIOS appliance does not support UTF-8 encoding for data that is configurable through the Infoblox CLI commands.

In general, the following items support UTF-8 encoding:

- All the predefined and user-defined extensible attributes.
- All the comment fields in Grid Manager.
- File name fields for FTP and TFTP backup and restore operations.
- The login banner text field. When you use the serial console or SSH, the appliance cannot correctly display the UTF-8 encoded information that you enter for the login banner.

**Note**: For data fields that do not support UTF-8 encoding, the appliance displays an error message when you use non-English characters.

### UTF-8 Support Limitations

The NIOS appliance has the following UTF-8 support limitations:

- Object names that have data restrictions due to their usage outside of the Infoblox database do not support UTF-8 encoding. For example, IP addresses and Active Directory domain names.
- When importing a database, most of the ASCII control characters cannot be encoded. This might cause failures in upgrades or database restore operations.
- Search is based on the Unicode standard. Depending on the language, you might not be able to perform a case-sensitive search.
- Binary data is encoded as text.
- UTF-8 encoding does not fully support regular expressions. It matches constant strings. However, It does not encode characters that are inside square brackets or followed by regular expressions such as “", ?, or +.
- You can use UTF-8 characters to authenticate both the User Name and Password through the Infoblox GUI, but not through the Infoblox CLI.
- You cannot use UTF-8 characters to name a custom DHCP fingerprint. For information about DHCP fingerprint detection, see Infoblox D HCP Fingerprint Detection.
Support for Internationalized Domain Names

The Infoblox Grid supports IDNs (Internationalized Domain Names) for DNS zones and resource records to provide the flexibility of specifying domain names in non-English characters.

An IDN is a domain name that contains a language-specific script or alphabet, such as Arabic, Chinese, Russian, Devanagari, or the Latin alphabet-based characters with diacritics, such as French. IDNs are encoded in multi-byte Unicode and are decoded into ASCII strings using a standardized mechanism known as Punycode transcription. For example, DNS Zone ‘xn--90anhdigczv.xn--p1ai’ in the punycode representation. In addition, the appliance has a built-in conversion tool to assist you in identifying and troubleshooting an IDN or the punycode representation of an IDN. For information about how to decode IDNs, see 4489220.

The appliance supports IDNs in certain fields. For more information, see 4489220. There are certain guidelines and limitations about IDN support. For more information, see 4489220.

Decoding IDNs and Encoding Punycode

You can encode non-English characters into punycode and decode punycode to obtain a domain name in its original character set. You can encode IDNs and decode punycode simultaneously. You can use special characters.

To encode non-English character set into punycode and decode punycode:

1. Select any tab in Grid Manager, and then click IDN Converter from the Toolbar.
2. In the IDN Converter wizard, complete the following:
   - Specify the domain name in the Unicode text box and click Convert to Punycode. The Punycode field displays the punycode representation of the domain name.
   - Specify the punycode representation of a domain name in the Punycode field and click Convert to Unicode. The Unicode field displays the domain name in its original character set.

   Note: You can use special characters in the Unicode and Punycode fields.

   - Click Clear to clear the entries. Note that when you click Clear for a specific conversion, the appliance clears only the error message that corresponds to that conversion.

3. Click Close.

IDN Supported Fields

The NIOS appliance supports IDNs in all domain name fields. For information, see IDN Support For DNS Zones. You can enter non-English characters in the domain name fields through Grid Manager and the Infoblox API. The NIOS appliance does not support IDNs for data that is configurable through the Infoblox CLI commands. You can use the punycode representation to configure data through the CLI commands.

The appliance supports IDNs in the following:

- You can use UTF-8 characters when defining your own hostname checking policy. For information, see Specifying Hostname Policies.
- You can use both IDNs and punycode to search for IDN data through Global Search. For information, see Global Search.
- Use smart folders to organize and monitor IDN data. However, if the content in a smart folder contains IDNs, then the punycode representation is not available. For information, see About Smart Folders.
- You can import data that contains IDNs in CSV format for the supported fields and objects using CSV import. For more information, see About CSV Import. For a list of supported record types and specific guidelines for creating a data file, refer to the Infoblox CSV Import Reference.
- The IPAM tab displays IDNs for DNS resource records associated with IP addresses, such as A records, AAAA records, hosts, and PTR records. For information, see About IP Address Management.
- The audit log entries are displayed in their original characters. The audit log contains IDN data as received by the appliance and as specified by the administrators. Note that the punycode representation generated by NIOS is not displayed in the audit log.
- When you upgrade from a previous NIOS release, the appliance converts all punycode to IDNs. If the conversion fails, the appliance retains the punycode representation to avoid upgrade failure. For information about upgrades, see Guidelines for Upgrading, Backing Up, and Restoring Data.
- When you restore a backup file from a previous NIOS release, the appliance converts all punycode to IDNs. If the conversion fails, the appliance retains the punycode representation to avoid failure to restore the database. For information, see Guidelines for Upgrading, Backing Up, and Restoring Data.
- If synchronized data between the appliance and Microsoft servers contains IDNs, the IDNs are preserved. For information, see Managing Microsoft DNS Servers.

IDN Support Limitations

The appliance has the following IDN support limitations:

- F5® load balancers does not support IDNs. The NIOS appliance does not encode punycode to IDNs for F5 load balancer related objects. Only the punycode representation is available.
- Multi-Grid configuration does not support IDNs.
- The Infoblox CLI does not support IDNs.
- If a resource record containing an IDN is added to the Infoblox Grid through DDNS updates, the domain name field displays the...
record name in UTF-8 encoded format. For more information, see Managing Resource Records.

- The following FQDNs does not support IDNs:
  - FQDN of an external DNS Server (direct or via name server group)
  - FQDN of a DNS root server
  - FQDN of a Microsoft server
  - FQDN of an Infoblox Grid Member
  - FQDN of an external authentication source (Active Directory, LDAP, OCSP, RADIUS, TACACS+)
  - FQDN of an NTP server
  - FQDN of an HSM SafeNet Module
  - FQDN of an email relay server
  - FQDN of a vSphere/ESX server
  - FQDN of a Kerberos Key Distribution Center

Using IDNs for Unsupported Objects

The appliance accepts only punycode entries for objects that do not support IDNs. To use IDNs for these objects, manually convert IDNs to punycode and use the punycode representation.

Use the punycode representation of IDNs for the following:

- When you configure domain names in forwarder servers, NXDOMAIN rulesets, blacklist rules, and DNS resolver search lists.
- When you configure domain names for DHCP and DHCPv6 services, including DDNS domain name, any DHCP options that accept domain names (host-name (12) string) or lists of domain names (domain-search (119) domain-list), and DHCPv6 options that accept domain names (dhcp6.fqdn (39) string) or lists of domain names (dhcp6.domain-search (24)) domain-list.
- When you add domains in the Inclusion list and Exclusion list. For information, see Excluding Domains From Query and Response Capture.
- When you configure rules for a local RPZ and RPZ feed. For information, see Configuring Local RPZs and Infoblox Threat Intelligence Feeds.

Displaying IDN Entries in Punycode

The appliance displays IDN entries in punycode for the following:

- The data of a zone for which an Infoblox Grid member is the secondary server.
- The CLI commands dig, ddns_add, ddns_delete, show dns, and set dns support punycode only. For information about CLI commands, refer to the Infoblox CLI Guide.
- All syslog entries generated by DNS.
- IDN data in database files is stored in punycode.
- The DNS cache of a Grid member that contains IDNs.
- The Reporting tab displays all report data that contains IDNs in punycode. For information, see Predefined Dashboards.

Chapter 2 Dashboards

Dashboards provide easy access to tasks and a quick overview to the status of your Grid and DNS, DHCP and IPAM services. This chapter contains the following sections:

- 4817236
  - The Tasks Dashboard
    - About Task Packs
    - The IPAM Task Pack
    - The NetMRI Task Pack
  - About Dashboard Templates
    - Adding Dashboard Templates
    - Modifying Dashboard Templates
    - Deleting Dashboard Templates
    - Assigning Dashboard Templates
  - Status Dashboards
    - Adding Widgets to Dashboards
    - Grid Status
    - Grid Upgrade Status
    - Member Status (System Status)
    - DNS Statistics
    - Ranges Over Threshold
    - IPv4 Failover Associations Status
    - DHCP Statistics
    - Network Statistics
    - Network Users - Active Users
    - IPv4 Networks Over Threshold
    - Port Status
    - Discovery Status
    - My Commands
The Dashboard is your home page on Grid Manager. It provides easy access to tasks and a quick view to the status of your Grid and core network services. Grid Manager provides the following dashboards:

- **Tasks**: The Tasks dashboard contains task packs that provide easy access to commonly performed tasks. A task pack is a collection of tasks that belong to a specific service or function, such as IPAM or Automation. For information, see [The Tasks Dashboard](#).
- **Status**: A status dashboard contains widgets from which you can view and manage DNS, DHCP, and IPAM status and data. You can configure multiple status dashboards for managing a large number of Grid members. For information, see [Status Dashboards](#).
- **Reporting Clustering Status**: The Reporting Clustering Status dashboard displays the reporting clustering status. This tab is displayed only if you have configured reporting clustering. For information, see [Reporting Clustering Status](#).

When you first log in to Grid Manager, the tasks dashboard is your home page. You can change your home page for subsequent logins. To change your home page:

1. Navigate to any tab in Grid Manager (except for the **Dashboards** tab).
2. Click **User Profile** from the Toolbar and complete the following In the **User Profile** dialog box:
   - **Default Dashboard**: Select **Status** or **Task** from the drop-down list.
3. Save the configuration.

Grid Manager displays the selected dashboard as your home page when you log in the next time.

### The Tasks Dashboard

The Tasks Dashboard provides easy access to commonly performed tasks, such as adding networks and adding host records. Tasks are grouped by service-specific task packs. You must install valid licenses on the appliance to see and perform specific tasks on the Tasks Dashboard. For information about the required licenses for IPAM tasks, see [4820092](#).

You must also have at least read-only permission to a task-related object to add or hide the task in its task pack. To execute a task, you must have the appropriate permissions to the member and objects that are related to the tasks. For example, to add a host record from the Tasks Dashboard, you must have at least read-only permission to the host records task and read/write permission to the zone and network in which the host records are created. For information about permissions, see [Administrative Permissions for Dashboard Tasks](#).

### About Task Packs

Grid Manager displays task packs, including the IPAM and NetMRI task packs, based on valid licenses installed on the appliance. To access the IPAM task pack, you must have valid DNS or DHCP license installed on the NIOS appliance. To access the Automation task pack, you must first set up an Infoblox NetMRI appliance, install the Automation Change Management license on the NIOS appliance, and register as a user. For information about how to activate the Automation task pack, refer to the [Infoblox NetMRI Administrator Guide](#).

**Note**: The Tasks Dashboard will not appear in the NIOS system if no task packs are licensed for the system. Some task packs will also have dependencies. For example, the NetMRI Task Pack licensing activates along with either the MS license or the NIOS DHCP/DNS combination license. Should either of those licenses be disabled for any reason, the NetMRI Tasks will also be disabled.

To use the Automation Task Pack, you must enable the NetMRI Tasks feature set and establish a working connection between the NIOS appliance and an Infoblox NetMRI appliance. See [4820092](#) for details. Each task in a task pack opens a workflow dialog in which you can create...
task-related objects without navigating through other tabs and editors in Grid Manager. Depending on the task you perform, Grid Manager displays task results in the Result page from which you can access newly created objects, such as networks and host records. Note that when a task takes longer than usual to complete, it becomes a long running task. For information about long running tasks, see About Tasks.

With valid licenses and proper registrations, Grid Manager displays the following task packs in the Tasks Dashboard:

- 4820092
- 4820092

The IPAM Task Pack

The IPAM task pack contains the following tasks:

- 4820092
- 4820092
- 4820092
- 4820092
- 4820092
- 4820092
- 4820092
- 4820092

Depending on your administrative permissions and the Dashboard template configuration, Grid Manager displays tasks you can access in specific task packs. You can configure your task packs by adding or hiding certain tasks. For information about Dashboard templates, see About Dashboard Templates.

To hide tasks in a task pack:

1. Click the Configure icon at the upper right corner of the task pack.
2. In the configuration panel, select the tasks you want to hide from the Active Tasks table. You can use SHIFT+click and CTRL+click to select multiple tasks.
3. Click the left arrow to move the selected tasks to the Available Tasks table.

Click the Configuration icon again to hide the configuration panel after you complete the modification.

Required Licenses for IPAM Tasks

Table 2.1 Required Licenses for IPAM Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Required Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Networks</td>
<td>DHCP or MSMGMT license</td>
</tr>
<tr>
<td>Add Hosts</td>
<td>DNS or DHCP license</td>
</tr>
<tr>
<td>Add Fixed Addresses</td>
<td>DHCP or MSMGMT license</td>
</tr>
<tr>
<td>Add A Record</td>
<td>DNS or MSMGMT license</td>
</tr>
<tr>
<td>Add CNAME Record</td>
<td>DNS or MSMGMT license</td>
</tr>
<tr>
<td>Add TXT Record</td>
<td>DNS or MSMGMT license</td>
</tr>
<tr>
<td>Add MX Record</td>
<td>DNS or MSMGMT license</td>
</tr>
</tbody>
</table>

For information about how to install licenses, see Managing Licenses.

Add Networks

You can create IPv4 and IPv6 networks from the Tasks Dashboard (either from scratch or from a network template that contains predefined properties). You can also create networks from the Data Management tab. For more information about IPv4 and IPv6 networks, see Configuring IPv4 Networks and Configuring IPv6 Networks.

To add networks from the Tasks Dashboard:

1. Click Add Networks in the IPAM task pack and complete the following in the Add Networks wizard:
   - Regional Internet Registry: This section appears only when support for RIR updates is enabled. For information about RIR, see RIR Registration Updates. Complete the following to create an RIR IPv4 network container or network:
     - Internet Registry: Select the RIR from the drop-down list. The default is RIPE. When you select None, the network is not associated with an RIR organization.
     - Organization ID: Click Select Organization and select an organization from the RIR Organization Selector dialog box.
     - Registration Status: The default is Not Registered. When adding an RIR allocated network, you can change this to Registered and select the Do not update registrations check box below. Note that when you select API as the communication method, the registration status will be updated automatically after the registration update is completed.
However, when you select Email as the communication method, the registration status will not be automatically updated. If you are creating a new network and the registration update is completed successfully, the status will be changed to Registered. If the update fails, the status will be changed to Not Registered. The updated status and timestamp are displayed in the Status of last update field in the IPv4 /IPv6 Network Container or IPv4/IPv6 Network editor.

- **Registration Action**: Select the registration action from the drop-down list. When you select Create, the appliance creates the IPv4 or IPv6 network and assigns it to the selected organization. When you select None, the appliance does not send registration updates to RIPE. When you are adding an existing RIR allocated network to NIOS, select None. When you are adding networks to an RIR allocated network (a parent network), select Create. Ensure that the parent network associated with an RIR organization already exists.

- **Do not update registrations**: Select this check box if you do not want the appliance to submit RIR updates to RIPE. By default, the appliance sends updates to the RIR database based on the configured communication method.

- **Network View**: This appears only when you have multiple network views. From the drop-down list, select the network view in which you want to create the network.

- **Protocol**: Select IPv4 to add IPv4 networks and IPv6 to add IPv6 networks.

- **Netmask**: Enter the netmask or use the netmask slider to select the appropriate number of subnet mask bits for the network.

- **Template**: Click Select Template to select a network template. When you use a template to create a network, the configuration of the template applies to the new network. If the template specifies a fixed netmask, you cannot edit the netmask in this dialog. You can click **Clear** to remove the template. For information about templates, see **About IPv4 Network Templates** and **About IPv6 Network Templates**.

- **Use Active Directory Sites**: This check box is displayed only if you install the Microsoft license. Click the Add icon to associate multiple Active Directory Sites with the network. When you click Add, the appliance displays the following:
  - **Active Directory Domain**: The Active Directory Domains that are synchronized from the Microsoft server. Click an Active Directory Domain that you want to associate. To search for a particular Active Directory Domain, specify the respective name and click **Go**. If there are multiple Active Directory Domains, the appliance displays the list of such domains by paging to the next page. You can use the page navigation buttons that are displayed at the bottom of this column to navigate through the Active Directory Domains. You can also refresh the values in the column using the Refresh icon.
  - **Active Directory Site**: The Active Directory Sites that are associated with the selected Active Directory Domain. Click an Active Directory Site that you want to associate with the network. To search for a particular Active Directory Site, specify the respective name and click **Go**. If there are multiple Active Directory Sites, the appliance displays the list of such sites by paging to the next page. You can use the page navigation buttons that are displayed at the bottom of this column to navigate through the Active Directory Sites. You can also refresh the values in the column using the Refresh icon.
  - **Click Add** to add the selected Active Directory Sites to the network or click **Cancel** to cancel the operation. The appliance displays these domains and sites in the respective columns. Click the x icon if you want to close the Active Directory Domains and Sites selector.
  - **Click the Delete icon to delete Active Directory Sites that are associated with the network.**

For more information about Active Directory Domains and Sites, see **About Active Directory Sites and Services**.

NIOS may execute discovery on the newly created network after you save your settings. When you create a network in NIOS, it inherits its discovery capabilities (whether or not it is immediately discovered, its polling settings, and any possible exclusions from discovery), from its parent network (if it has one) or its network container. If the new network is a parent network, it inherits its discovery member selection and Enable Discovery action must be defined by the user.

- **Networks**: Do one of the following to add new networks:
  - Click the Add icon to create a new network.
  - For IPv4 networks: Grid Manager adds a row to the table. Enter the network address in the **Network** field. Click the Add icon to add another network. You can also select a network and click the **Delete** icon to delete it.
  - For IPv6 networks: If you are adding a network for a previously defined global IPv6 prefix, you can select the prefix from the **IPv6 Prefix** drop-down list. The default is **None**, which means that you are not creating an IPv6 network for a previously defined subnet route. If you have defined a global prefix at the Grid level, the default is the global prefix value. Click **Add** and Grid Manager adds a row to the table. Enter the network address in the **Network** field. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2001:0db8:0000:0000:0000:0102:0304 can be shortened to 2001:db8::0102:0304. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one double colon to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2001:0db8:0000:0000:0000:0102:0304 can be shortened to 2001:db8::0102:0304. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one.
  - Click the Next Available icon to have the appliance search for the next available network. For more information about the next available network, see **About the Next Available Network or IP Address**. Complete the following in the Next Available Networks section:
    - **Create new network(s) under**: Enter the network container in which you want to create the new network. When you enter a network that does not exist, the appliance adds it as a network container. When you enter a network that is part of a parent network, the parent network is converted into a network container if it does not have a member assignment or does not contain address ranges, fixed addresses, reservations, shared networks, and host records that are served by DHCP. When you enter a network that has a lower CIDR than an existing network, the appliance creates the network as a parent network and displays a message indicating that the newly created network overlaps an existing network. You can also click **Select Network** to select a specific network in the **Network Selector** dialog box. For information about how the appliance searches for the next available network, see **Obtaining the Next Available**.

Copyright ©2019, Infoblox, Inc. All right reserved.
• **Number of new networks:** Enter the number of networks you want to add to the selected network container. Note that if there is not enough network space in the selected network to create the number of networks specified here, Grid Manager displays an error message. The maximum number is 20 at a time. Note that when you have existing networks in the table and you select one, the number you enter here includes the selected network.

• **Click Add Next** to add the networks. Grid Manager lists the networks in the table. You can click **Cancel** to reset the values.

**Note:** You must click **Add Next** to add the network container you enter in the **Next Available Networks** section. If you enter a network in the **Next Available Networks** section and then use the Add icon to add another network, the appliance does not save the network you enter in the **Next Available Networks** section until you click **Add Next**.

- **Extensible Attributes:** Click the Add icon to enter extensible attributes. Grid Manager adds a row to the table each time you click the Add icon. Select the row and the attribute name from the drop-down list, and then enter the value. All inheritance attributes which can be inherited from a parent object will be automatically inherited when you add a network. Inheritable extensible attributes that are required are automatically displayed. Optional extensible attributes that are not inheritable are not automatically displayed. For more information about extensible attributes, see **Using Extensible Attributes**.

- If you are adding an RIR network, the RIR network attribute table appears. For information about these attributes and how to enter them, see **RIR Network Attributes**.

**Preview RIR Submissions:** Click this to view the updates before the appliance submits them to the RIPE database. This button is enabled only when the registration action is **Create**, **Modify**, or **Delete**, and the **Do not update registrations** check box is not selected.

2. Save the configuration.

or
Click the **Schedule** icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, click **Later** and enter a date, time, and time zone. For information, see **About Extensible Attributes**.

The appliance saves the networks you just created, and Grid Manager displays them in the Result page. When you click a newly created network on this page, Grid Manager displays the **IP Map** panel from which you can view detailed information about the network. For information about the IP Map panel, see **IP Map**.

You can also add and modify other information about the networks you just created. For information about modifying network information, see **Managing IPv4 DHCP Data** and **Managing IPv6 DHCP Data**.

**Add Hosts**

Host records provide a unique approach to the management of DNS, DHCP, and IPAM data. By using host records, you can manage multiple DNS records and DHCP and IPAM data collectively, as one object on the appliance. You can add IPv4 and IPv6 addresses to host records from the Tasks Dashboard or the **Data Management** tab. Note that when you add a host record from the Tasks Dashboard, they are configured only for DNS. For more information about Infoblox host records, see **About Host Records**.

To add host records from the Tasks Dashboard:

1. Click **Add Hosts** in the IPAM Task Pack and complete the following in the **Add Hosts** wizard:

   - **Network View:** Appears only when you have multiple network views. From the drop-down list, select the network view in which you want to create the host record.

   - **Zone Name:** Click **Select** to select a DNS zone from the **Zone Selector** dialog box.

   - **Exclude from Network Discovery** and **Immediate Discovery.** When creating the new Host record, you can direct NIOS to immediately discover the host, or to exclude it from network discovery. By default, the Add Hosts task enables immediate discovery.

   - **DNS View:** Displays the DNS view of the selected zone.

   - **Hosts:** Do one of the following to add a host record:

     - **Name:** Enter the name of the host record.

     - **Zone:** Displays the DNS zone you select in **Zone Name.** When you enter a different zone here, the appliance displays an error message.

     - **Address:** Enter the IP address you want to associate with this host record.

   or

   Click the Next Available icon to have the appliance search for the next available IP address for the host record. For information about the next available IP address, see **About the Next Available Network or IP Address**. Complete the following in the Next Available IP section:

   - **Create new host addresses under:** Click **Select** to select the network or address range in the **Network/Range Selector** dialog box from which you want the appliance to search for the next available IP address for this host record.

   - **Number of new host addresses:** Enter the number of host addresses. Note that if there is not enough space in the selected network or address range to create the number of host addresses specified here, Grid Manager displays an error message. The maximum number is 20 at a time. Note that when you have existing host addresses in the table and you select one, the number you enter here includes the selected host address.

   - **Click Add Next** to add the IP addresses to their corresponding hosts. Grid Manager lists the host addresses in the table. Ensure that you enter a name for each host record.

   - **Extensible Attributes**

     - **Apply to all above hosts:** Select this to associate extensible attributes with all hosts that you have defined. This is
selected by default. You can define and associate multiple extensible attributes with multiple hosts at once.

- **Apply to selected host**: Select this to associate extensible attributes with the selected host only. Note that when you select this option for another host in the list, the **Extensible Attributes table** is refreshed for you to associate a different set of extensible attributes with the selected host.

- **Extensible Attributes table**: Click the Add icon to enter extensible attributes. The appliance adds a row to the table each time you click the Add icon. Select the row and the attribute name from the drop-down list, and then enter the value. All inheritance attributes which can be inherited from a parent object will be automatically inherited when you add a host. Inheritable extensible attributes that are required are automatically displayed. Optional extensible attributes that are not inheritable are not automatically displayed. For more information about extensible attributes, see *About Extensible Attributes*.

2. Save the configuration.

Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, click **Later** and enter a date, time, and time zone. For information about how to schedule a task, see *Scheduling Tasks*.

The appliance saves the host records you just created, and Grid Manager displays them in the Result page. When you click a newly created host on this page, Grid Manager displays the **Data Management -> DNS -> Zones** tab from which you can view information about the host record. You can also add and modify other information about the host records. For information about modifying host information, see *About Host Records*.

### Add Fixed Addresses

You can add IPv4 and IPv6 fixed addresses from the Tasks Dashboard or from the **Data Management** tab. For more information about fixed addresses, see *Configuring IPv4 Fixed Addresses* and *Configuring IPv6 Fixed Addresses*.

To add fixed addresses from the Tasks Dashboard:

1. Click **Add Fixed Addresses** in the IPAM task pack and complete the following in the **Add Fixed Addresses** wizard:
   - **Network View**: This appears only when you have multiple network views. From the drop-down list, select the network view in which you want to create the fixed address.
   - **Protocol**: Select **IPv4** to add IPv4 addresses and **IPv6** to add IPv6 addresses.
   - **Template**: Click **Select Template** to select a fixed address template. When you use a template to create a fixed address, the configuration of the template applies to the new fixed address. You can also click **Clear** to remove the template. For information about templates, see *About DHCP Templates*.
   - **Exclude from Network Discovery** and **Immediate Discovery**: When creating the new fixed address, you can direct NICs to immediately discover the device associated with the fixed address, or to exclude it from network discovery. By default, the Add Fixed Addresses task enables immediate discovery.
   - **Addresses**: Do one of the following to add fixed addresses:
     - Create **new fixed addresses under**: Click **Select** to select the network or address range in the *Network/Range Selector* dialog box from which you want the appliance to search for the next available IP address for this fixed address.
     - **Number of new fixed addresses**: Enter the number of fixed addresses you want to add to the selected network or address range. Note that if there is not enough space in the selected network or address range to create the number of fixed addresses specified here, Grid Manager displays an error message. The maximum number is 20 at a time. Note that when you have existing fixed addresses in the table and you select one, the number you enter here includes the selected fixed address.
     - **Click Add Next** to add the fixed addresses. The appliance lists the fixed addresses to the table. Ensure that you enter the MAC address or DUID for each fixed address.
   - **Extensible Attributes table**: Click the Add icon to enter extensible attributes. The appliance adds a row to the table each time you click the Add icon. Select the row and the attribute name from the drop-down list, and then enter the value. All inheritance attributes which can be inherited from a parent object will be automatically inherited when you add a fixed address. Inheritable extensible attributes that are required are automatically displayed. Optional extensible attributes that are not inheritable are not automatically displayed. For more information about extensible attributes, see *About Extensible Attributes*.

2. Save the configuration.

Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, click **Later** and enter a date, time, and time zone. For information, see *Scheduling Tasks*.

The appliance saves the fixed addresses you just created, and Grid Manager displays them in the Result page. When you click a newly created fixed address on this page, Grid Manager displays the **Data Management -> IPAM -> IP Map** or **List** tab from which you can view information about the fixed address. You can also add and modify other information about the fixed addresses you just created. For more information about modifying fixed address information, see *Managing IPv4 DHCP Data* and *Managing IPv6 DHCP Data*. 

---

Copyright ©2019, Infoblox, Inc. All right reserved.
Add A Record

An A (address) record is a DNS resource record that maps a domain name to an IPv4 address. You can add an A record from the Tasks Dashboard or from the Data Management tab. For more information about managing A records, see Managing A Records.
To add networks from the Tasks Dashboard:

1. Click Add A Record in the IPAM task pack and complete the following in the Add A Record wizard:
2. In the Add A Record wizard, do the following:
   • Name: If Grid Manager displays a zone name, enter the hostname that you want to map to an IP address. The displayed zone name can either be the last selected zone or the zone from which you are adding the host record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box and then enter the hostname. The name you enter is prefixed to the DNS zone name that is displayed, and the complete name becomes the FQDN (fully qualified domain name) of the host. For example, if the zone name displayed is corpxyz.com and you enter admin, then the FQDN becomes admin.corpxyz.com. Ensure that the domain name you enter complies with the hostname restriction policy defined for the zone. To create a wildcard A record, enter an asterisk * in this field.
   • DNS View: This field displays the DNS view to which the DNS zone belongs.
   • Shared Record Group: This field appears only when you are creating a shared record from the Data Management tab. Click Select Shared Record Group. If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the Shared Record Group Selector dialog box. You can use filters or the Go to function to narrow down the list.
   • Hostname Policy: Displays the hostname policy of the zone.
   • In the IP Addresses section, click the Add icon and do one of the following:
     • Select Add Address to enter the IPv4 address to which you want the domain name to map.
     or
     • Select Next Available IPv4 to retrieve the next available IPv address in a network.
     • If the A record is in a zone that has associated networks, the Network Selector dialog box lists the associated networks. If the zone has no network associations, the Network Selector dialog box lists the available networks. When you select a network, Grid Manager retrieves the next available IPv address in that network.
     • Comment: Optionally, enter additional information about the A record.
     • Create associated PTR record: Select this option to automatically generate a PTR record that maps the specified IP address to the hostname. To create the PTR record, the reverse-mapping zone must be in the database.
     • Disable: Select this check box to disable the record. Clear the check box to enable it.
3. Click Next to define extensible attributes. For information, see Using Extensible Attributes.
4. Save the configuration or click the Schedule icon at the top of the wizard to schedule this task. For information about how to schedule a task, see Scheduling Tasks.
5. Click Restart if it appears at the top of the screen.

Add CNAME Record

A CNAME record maps an alias to a canonical name. You can use CNAME records in both IPv4 forward- and IPv4 reverse-mapping zones to serve two different purposes. (At this time, you cannot use CNAME records with IPv6 reverse-mapping zones.) For more information about CNAME records, see Managing CNAME Records.
To add a CNAME record from the Tasks Dashboard:

1. Click Add CNAME Record in the IPAM task pack and complete the following in the Add CNAME Record wizard:
   • Network View: This appears only when you have multiple network views. From the drop-down list, select the network view in which you want to create the CNAME record.
   • Alias: Click Select Zone to select a DNS zone from the Zone Selector dialog box. If you have only one zone, Grid Manager displays the zone name here when you click Select Zone. Enter the alias for the canonical name. For an IPv4 reverse-mapping zone, enter the host portion of an IP address. For example, if the full IP address is 10.1.1.1 in a network with a 25-bit netmask, enter 1. (The 10.1.1.0/25 network contains host addresses from 10.1.1.1 to 10.1.1.255. The network address is 10.1.1.0, and the broadcast address is 10.1.1.255.)
   • DNS View: Displays the DNS view of the selected zone.
   • Shared Record Group: This field appears only when you are creating a shared record from the Data Management tab. Click Select Shared Record Group. If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the Shared Record Group Selector dialog box. You can use filters or the Go to function to narrow down the list.
   • Canonical Name: This field displays the domain name of either the current zone or the last selected zone. To add a CNAME record to a forward-mapping zone, enter the complete canonical (or official) name of the host. To add a CNAME record to a reverse-mapping zone, enter host_ip_addr.prefix.network.in-addr.arpa (host IP address + 2317 prefix + network IP address + in-addr.arpa). For example, enter 1.0.25.1.1.0.in-addr.arpa. This IP address must match the address defined in the PTR record in the delegated child zone.
   • Comments: Enter useful information about this record.
   • Disable: Select the check box to disable the record without deleting its configuration. Clear the check box to enable the record.
2. Save the configuration, or click Next to define extensible attributes. For information about extensible attributes, see Using Extensible Attributes.
3. Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, click Later and enter a date, time, and time zone. For information, see Scheduling Tasks.
Click **Restart** if it appears at the top of the screen.

You can also add and modify other information about the CNAME record you just created. For more information about modifying the CNAME record, see *Modifying, Disabling, and Deleting Host and Resource Records*.

### Add TXT Record

A TXT (text record) record contains supplemental information for a host. For example, if you have a sales server that serves only North America, you can create a text record stating this fact. You can create more than one text record for a domain name. You can add a TXT record from the Tasks Dashboard or the **Data Management** tab. For more information about TXT records, see *Managing TXT Records*.

To add TXT records from the Tasks Dashboard:

1. Click **Add TXT Record** in the IPAM task pack and complete the following in the **Add TXT Record** wizard:
   - **Network View** - This appears only when you have multiple network views. From the drop-down list, select the network view in which you want to create the TXT record.
   - **Name** - If Grid Manager displays a zone name, enter the name to define a TXT record for a host or subdomain. If no zone name is displayed or if you want to specify a different zone, click **Select Zone**. When there are multiple zones, Grid Manager displays the **Zone Selector** dialog box. Click a zone name in the dialog box. Then, enter the TXT record name. The appliance prefixes the name you enter to the domain name of the selected zone. For example, if you want to create a TXT record for a web server whose host name is www2.corpxyz.com and you define the TXT record in the corpxyz.com zone, enter **www2** in this field. To define a TXT record for a domain whose name matches the selected zone, leave this field empty. The appliance automatically adds the domain name (the same as the zone name) to the TXT record. For example, if you want to create a TXT record for the corpxyz.com domain and you selected the corpxyz.com zone, leave this field empty.
   - **DNS View** - Displays the DNS view of the selected zone.
   - **Shared Record Group** - This field appears only when you are creating a shared record from the **Data Management** tab. Click **Select Shared Record Group**. If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the **Shared Record Group Selector** dialog box. You can use filters or the **Goto** function to narrow down the list.
   - **Text** - Enter the text that you want to associate with the record. It can contain substrings of up to 255 bytes, up to a total of 512 bytes. Additionally, if you enter leading, trailing, or embedded spaces in the text, add quotes around the text to preserve the spaces. For example: " v=spf1 include:corp200.com -all "
   - **Comments** - Enter useful information about this record.
   - **Disable** - Select the check box to disable the record without deleting its configuration. Clear the check box to enable the record.

2. Save the configuration, or click **Next** to define extensible attributes. For information, see *About Extensible Attributes*.

Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, click **Later** and enter a date, time, and time zone. For information, see *Scheduling Tasks*.

3. Click **Restart** if it appears at the top of the screen.

### Add MX Record

An MX (mail exchanger) record maps a domain name to a mail exchanger. A mail exchanger is a server that either delivers or forwards mail. You can specify one or more mail exchangers for a zone, as well as the preference for using each mail exchanger. A standard MX record applies to a particular domain or subdomain. You can add an MX record from the Tasks Dashboard or the **Data Management** tab. For more information about MX records, see *Managing MX Records*.

To add MX records from the Tasks Dashboard:

1. Click **Add MX Record** in the IPAM task pack and complete the following in the **Add TXT Record** wizard:
   - **Network View** - This appears only when you have multiple network views. From the drop-down list, select the network view in which you want to create the MX record.
   - **Mail Destination** - If Grid Manager displays a zone name, enter the mail destination here. If no zone name is displayed or if you want to specify a different zone, click **Select Zone**. When there are multiple zones, Grid Manager displays the **Zone Selector** dialog box. Click a zone name in the dialog box, and then enter the mail destination. If you want to define an MX record for a domain whose name matches the zone you selected, leave this field blank. Grid Manager automatically adds the domain name (the same as the zone name) to the MX record. For example, if you want to create an MX record for a mail exchanger serving the corpxyz.com domain and you selected the corpxyz.com zone, and leave this field empty. If you want to define an MX record for a subdomain, enter the subdomain name. The appliance prefixes the name you enter to the domain name of the selected zone. For example, if you want to create an MX record for a mail exchanger serving site1.corpxyz.com—a subdomain of corpxyz.com—and you define the MX record in the corpxyz.com zone, enter site1 in this field. If you want to define an MX record for a domain and all its subdomains, enter an asterisk ("*") to create a wildcard MX record.
   - **DNS View** - Displays the DNS view of the selected zone.
   - **Shared Record Group** - This field appears only when you are creating a shared record from the **Data Management** tab. Click **Select Shared Record Group**. If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the **Shared Record Group Selector** dialog box. You can use filters or the **Goto** function to narrow down the list.
   - **Host Name Policy** - Displays the hostname policy of the selected zone. Ensure that the hostname you enter complies with the hostname restriction policy defined for the zone.
• **Mail Exchanger:** Enter the fully qualified domain name of the mail exchanger.
• **Preference:** Select an integer from 10 to 100, or enter a value from 0 to 65535. The preference determines the order in which a client attempts to contact the target mail exchanger.
• **Comment:** Enter useful information about this record.
• **Disable:** Select the check box to disable the record without deleting its configuration. Clear the check box to enable the record.

2. Save the configuration, or click **Next** to define extensible attributes. For information, see **About Extensible Attributes**.

or
Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, click **Later** and enter a date, time, and time zone. For information about scheduling tasks, see **Scheduling Tasks**.

3. Click **Restart** if it appears at the top of the screen.

**CSV Import**

You can access **CSV Import Manager** and perform CSV imports, manage import jobs, and view import status. You can perform CSV imports from the Task Dashboard and the Toolbar. You can also click **CSV Import Manager**, which allows for importing of data, managing import jobs, and viewing import status.

You can click **New CSV import job** icon in the **CSV Job Manager** wizard to import a CSV file to the database. You can also verify the content in your CSV file before replacing the content of the database with the content in the imported CSV file. For detailed information about the CSV import feature, see **About CSV Import**.

**Enabling the NetMRI Tasks**

The NetMRI Tasks pack requires the configuration, licensing and connection of an Infoblox NetMRI appliance to support automation tasks. Should two superusers be logged in to the NIOS system and one superuser enables the NetMRI Tasks pack on their console, the other superuser will not see the task pack on their console until their next login; the **Disable NetMRI Tasks** from the Configure icon menu shows the correct state.

You install the NetMRI appliance into the managed network, ensuring the appliance is reachable by the NIOS Grid Master. After this is accomplished, you register the NetMRI appliance with NIOS.

1. Click the **Configure** icon at the top right corner of the **Tasks** page.
2. Choose **Enable NetMRI Tasks**.
   The Enable NetMRI Tasks dialog box appears, requesting verification of your action:
   - **Are you sure you want to proceed?**
3. Click **Yes** to enable the NetMRI Tasks set.
   After a moment, the NetMRI Tasks panel appears.

**Disabling NetMRI Tasks**

Should you need to disable the NetMRI Tasks pack, do the following:

1. Click the **Configure** icon at the top right corner of the **Tasks** page.
2. Choose **Disable NetMRI Tasks**.
   The Disable NetMRI Tasks dialog box appears, requesting verification of your action:
   - **Are you sure you want to proceed?**
3. Click **Yes** to disable the NetMRI Tasks pack.

**Registering NetMRI with NIOS**

You must register a NetMRI appliance with NIOS to support the NetMRI Tasks. This registration is done directly on the NIOS system. You need the admin account and password for the NetMRI appliance and its hostname or IP address.

Note that when you register NetMRI with a NIOS HA pair, you can register only one interface at a time. Use the IP address of the LAN1 interface, not the VIP address, for registration. When an HA failover occurs, the NetMRI registration is disabled. You can register the NetMRI appliance again after the failover.

1. From the **Dashboards** tab, select the **Tasks** tab.
2. At the top right corner of the Automation Tasks panel, click the **Configure** icon -> **NetMRI Registration**.

3. In the **NetMRI Registration** dialog, do the following:
   a. Enter the IP address or resolved host name of the NetMRI appliance supporting the Automation task pack.
   b. Enter the **Admin Password**.
This information is specific to the Infoblox NetMRI appliance supporting the Automation tasks in NIOS.

4. Click **Register** to commit settings.

**Note:** After you successfully register a NetMRI appliance with NIOS, you can use the Ecosystem > Cisco ISE Endpoint feature without having to install the Network Insight license. This enables you to enhance identity management across devices and applications that are connected to your network routers and switches. You can monitor domain users, the IP addresses they log on to, the login status, and the time duration of their current status in the IPAM tab. For information about how to collect user and device information from Cisco ISE, see [Cisco ISE Integration](#).

After registration, the **NetMRI Registration** menu item changes to read **NetMRI Deregistration** to support disconnecting from the NetMRI appliance.

You can also start NetMRI from the NIOS Dashboards page.

1. From the Dashboard tab, select the Tasks tab.
2. In the Automation Tasks pane, click the down arrow gadget and select **Launch NetMRI**.

NetMRI launches in a new browser tab.

To check on script executions, go to Configuration Management -> Job Management side tab -> Scripts and check the Last Run column. The NIOS Task Viewer (see 4820092) also provides the log history of automated jobs.

---

**The NetMRI Task Pack**

The NetMRI task pack contains the following tasks:

- 4820092
- 4820092
- 4820092
- 4820092
- 4820092

Depending on your administrative permissions, Grid Manager displays tasks you can access in specific task packs. You can configure your task packs by adding or hiding certain tasks.

To hide tasks in a task pack:

1. Click the Configure icon at the upper right corner of the task pack.
2. In the configuration panel, select the tasks you want to hide from the Active Tasks table. You can use SHIFT+click and CTRL+click to select multiple tasks.
3. Click the left arrow to move the selected tasks to the Available Tasks table.

Click the Configuration icon again to hide the configuration panel after you complete the modification.

**NetMRI Task Options**

Tasks allow the assignment of job scripts to change and expand task functionality. These scripts reside on the NetMRI appliance and must be readable by the NIOS system to run the automation tasks. You can also select different scripts to execute for automation tasks that provide that feature in NIOS. Three NetMRI tasks allow for the choosing of non-default scripts for task operation:

- 4820092
- 4820092
- 4820092

**Network Provisioning Task**

The Network Provisioning task runs in two modes: a basic mode with a much shorter list of configuration options, and a more complex mode that provides detailed configuration for provisioning a network, including the use of NIOS network views, extensible attributes and network templates. New networks can be provisioned on routed networks and on switched networks. In the latter case, you can specify the new VLAN number and VLAN name for provisioning, along with the Device Group Device and Interface. The Device Group values are taken from the Device Groups defined on the NetMRI appliance from which NIOS obtains its data.

Network Provisioning supports two types of networks: **IPv4**, in which the new network is IPv4 only, and **IPv4 and IPv6**, in which the new network runs both protocol stacks.

**Simple vs. Complex Provisioning**

Use of a Network View determines whether you use the simple or detailed views of provisioning a network. A network view is a single routing domain with its own networks and shared networks. In NIOS, all networks must belong to a network view. You can manage networks in one network view independently of other network views. Because network views are mutually exclusive, the networks in each view can have
overlapping address spaces with multiple duplicate IP addresses without impacting network integrity. Also, the same network segment can be present in multiple network views. When you create a new network, you select one view in which to place it, and preserve those values to apply to another view.

You also have the option to provision a single network segment without recourse to NIOS network views. The simple network provisioning option (accessible by simply clicking the IPv4 tool at the top of the Network Provisioning dialog box) allows you to specify as few as three values to configure a network.

The NIOS system also provides a default network view, which appears as an option for network provisioning.

If a single network view is configured in NIOS, you will not see a Network View option in the Network Provisioning task.

Applying Extensible Attributes

Extensible attributes are associated with a specific network view, and are referenced by the Network Provisioning task. Should you configure a new network using a network view, you may need to consider the application of extensible attributes to the new network (they are not automatically applied, but will appear in the Network Provisioning dialog if those attributes are defined in the chosen Network View). Extensible attributes are generally defined for descriptive and tracking purposes in the network. A network view may have attributes such as Building, Country, Region, Site, State or VLAN, for example. Attributes are defined for network views in NIOS but are not defined by the NetMRI appliance. If the NIOS system supports only a single network view, no View selections are made for the purposes of network provisioning.

Required settings for provisioning a new network will show a red asterisk * by the option name. To perform an automatic network provisioning task:

1. From the Dashboards tab, select the Tasks tab -> Network Provisioning.
2. Select the network Type for provisioning: IPv4 or IPv4andIPv6.
3. To configure IPv4 provisioning:
   a. Enter the Parent Network value (or click Select Network to choose the parent network from a list if using a Network View).
   b. Choose the Network Template from the drop-down list if one is provided by the chosen Network View. The Network template is otherwise optional.
   c. Drag the Netmask slider to the required CIDR mask bit depth (1-32).
   d. In the New Network field, enter the IP prefix for the new network.
   e. In the Router Address field, enter the IP address for the router interface.
   f. Select any Extensible Attributes in the list if they are provided; otherwise, you can create new ones by clicking Add and choosing the Attribute Name, Value and the Required setting.
4. To configure IPv6 provisioning:
   a. Enter the Parent Network value (or click Select Network to choose the parent network from a list if using a Network View).
   b. Choose the Network Template from the drop-down list if one is provided by the chosen Network View. The Network template is otherwise optional.
   c. Drag the Netmask slider to the required CIDR mask bit depth (1-32).
   d. In the New Network field, enter the IP prefix for the new network.
   e. In the Router Address field, enter the IP address for the router interface.
   f. Select any Extensible Attributes in the list if they are provided; otherwise, you can create new ones by clicking Add and choosing the Attribute Name, Value and the Required setting.
5. Enter the required name value in the Interface Hostname field. (Examples include "eth0" and "serial0.")
6. Select the DNS Zone under which the hostname operates.
7. Choose a device group from the Device Group drop-down list.
8. From the Device drop-down list, choose the switch or router on which the network will originate.
9. If the selected device is a router, the VLAN Number and VLAN Name fields will be disabled.
10. From the Interface list, choose the interface to which the network will be reassigned. The drop-down list contains all the interfaces from the chosen network device, and also shows the ports’ respective states (up/down, up/up and so on).
    
    If an interface shows Routed or Switched, it cannot be selected for provisioning as it is already being used as part of an active network.
11. If the chosen device is a switch, enter the new VLAN Number on which the new network segment runs.
12. If the chosen device is a switch, enter the new VLAN Name on which the new network segment runs.
13. Click Provision Network to commit settings.

The network provisioning task provides several configuration options that affect how the task operates.

Hostname provisioning for interfaces is useful for troubleshooting purposes in the network, usually to ensure that an admin knows which router interface they are connecting through to communicate with the device. The hostname value is actually provisioned from within the Network

Defining Options for the Network Provisioning Task

The Network Provisioning task provides several configuration options that affect how the task operates.

Hostname provisioning for interfaces is useful for troubleshooting purposes in the network, usually to ensure that an admin knows which router interface they are connecting through to communicate with the device. The hostname value is actually provisioned from within the Network

Job History and view details about provisioning jobs and other jobs that execute as a result of NIOS-based automation tasks.

When you select a device, the system sends the configuration request to the NetMRI appliance and displays the task configuration sequence. You can start NetMRI from the registered NetMRI appliance to check job execution.

If a single network view is configured in NIOS, you will not see a Network View option in the Network Provisioning task.
Provisioning task. Enabling the Hostname Required? check box sets the NetMRI appliance to provision the network with hostnames applied to the router interfaces for easier identification.

Network provisioning requires that the system know exactly which IP address the gateway for the network will reside. For provisioning most networks, an Offset value of 1 indicates that the provisioned network gateway IP address ends with the host address of ...1, as in 192.168.1.1. An Offset value of 1 will be far the most common value for provisioning networks. Specifying an offset value other than 1 indicates that the gateway IP is a specified number of host values from the prefix address of the network. For example, setting an IPv4 Gateway Address Offset of 12 indicates that the IP for the gateway ends in *...12, as in 10.1.1.12. Offsets work the same way for any size network: for an example such as 10.1.1.64/26, and an offset of 12, the provisioned gateway IP would be 10.1.1.76. Make sure the defined offset value lies within the addressable boundaries of the provisioned network!

The same principles also apply for IPv6 networks, except that the IPv6 value is entered manually in hexadecimal instead of being selected from a drop-down list. Most provisioned IPv6 networks will use a /64 network address.

You can also select a different script from the default for the Network Provisioning task. To define settings for the Network Provisioning automated task:

1. From the Dashboards tab, select the Tasks tab. Under the Network Provisioning task, click the settings icon on the top right.
2. If the provisioning process requires a hostname, enable the Hostname Required? check box. (The network interface hostname ("eth0," "serial0") and the Zone that it belongs to are defined in the Network Provisioning task.)
3. Choose a gateway offset value from the IPv4 Gateway Address Offset drop-down list. If no value is selected, the offset value defaults to 1 for the provisioned network address.
4. If an IPv6 offset is required for provisioning an IPv6 network or for provisioning a network that supports both IPv4 and IPv6 addressing, enter the IPv6 Gateway Address Offset value in hexadecimal. If no value is entered, the offset value defaults to 0000.0000.0000.0001 for the provisioned network address, indicating an offset value of 1 for the gateway IP address.
5. In the Script Name dropdown, choose the script that you wish to run for the Port Activation task. The scripts are located on the Trinzic Automation 4000 appliance, and referenced for use by NIOS. By default, the bundled Port Activation script is selected.
6. Click Save to commit settings.
7. Click Cancel to close the dialog.

The system sends the request to the NetMRI appliance and displays a Provisioning Network Config updated notification message.

Using the Port Activation Automation Task

The Port Activation task provides a central console on which the interfaces for any device anywhere in the managed network can be conveniently enabled or disabled. Ports can be taken administratively Up or Down using this task, and all interfaces on a selected device can be activated or deactivated with a series of mouse clicks.

1. From the Dashboards tab, select the Tasks tab ➔ Port Activation.
2. Choose the Device Group from the drop-down list.
3. From the Device drop-down list, choose the network device on which port activation will be executed.
   - The Interfaces table lists all interfaces on the current device. The VLAN and VLAN Name columns list the VLAN assigned to each port (VLAN 1/Default resides on all ports without an explicit VLAN assignment). The OP Status column will show the current state of each interface.
4. Scroll down the table to locate the interface(s) you want to activate.
5. From the Admin Status column, select Up (or Down) from the drop-down list for the chosen interface.
6. Set any other interfaces on the current device based on your assigned task.
7. Click Apply to commit settings.

The system sends the request to the NetMRI appliance and displays the task configuration sequence. The Port Activation task will also write the full running configuration to memory, making it the saved configuration. If the user made a change to the running configuration, in parallel with the port activation change, and did not save it, those changes will also be saved.

Specifying a Port Activation Script

The Port Activation task provides a central console on which the interfaces for any device in the managed network can be conveniently activated. Ports can be taken administratively Up or Down using this task, and all interfaces on a selected device can be activated or deactivated with a series of mouse clicks.

The NetMRI appliance provides the ability to create new automation scripts for many purposes. You may, for example, wish to create a new Port Activation script and use that as an automation task.

To select a different script from the default choice in the software:

1. From the Dashboards tab, select the Tasks tab. Under the Port Activation task, click the settings icon.
2. For Port Activation Options, choose a new script from the Script Name drop-down list. The scripts are located on the Trinzic Automation 4000 appliance, and automatically referenced for use by NIOS. By default, the bundled Port Activation script is selected.
3. Click Save to commit settings.

The system sends the request to the NetMRI appliance and displays a notification message.

VLAN Reassignment

VLANs can be reassigned to new interfaces on individual L2/L3 switches in the managed network. A VLAN can have a path across several
switches; when you make changes on a given switch, make sure that the path is maintained.

To ensure end-to-end connectivity, you may need to change VLAN port assignments on more than one switch in the path. This feature operates with the VLAN Trunking Protocol (VTP). VLAN switching is changed across one port per switch at a time. Should you need to change VLAN assignments across more than one switch in the path, plan accordingly.

VLANs must already be configured on the switch(es) being changed, and be detected by the NetMRI appliance.

1. From the Dashboards tab, select the Tasks tab -> VLAN Reassignment.
2. Begin by selecting the Device Group from the drop-down list. For VLAN Reassignments, you typically choose the Switching device group.
3. From the Device drop-down list, choose the switch on which port reassignment will be executed.
4. From the Port list, choose the interface to which the VLAN will be reassigned. The Port list also shows the Administrative and Operational states of each interface on the current device (Administratively Up/Operationally Down, for example.)

Note: You can reassign a VLAN to a port that is operationally or administratively Down. The Current VLAN value will show the VLAN to which the selected interface is currently assigned.

5. Choose the new VLAN value for port reassignment from the New VLAN drop-down list.
6. Click Move VLAN to commit settings.

The system sends the configuration request to the NetMRI appliance and displays the task configuration sequence.

The VLAN Reassignment task will also write the full running configuration to memory, making it the saved configuration. If the user made a change to the running configuration, in parallel with the port activation change, and did not save it, those changes will also be saved.

Assigning a New Script to the VLAN Reassignments Task

The NetMRI appliance provides the ability to create new automation scripts for many purposes. You can create and assign a new VLAN Reassignment script and use that for the automation task.

To select a different script from the default choice in the software:

1. From the Dashboards tab, select the Tasks tab. Under the VLAN Reassignment task, click the settings icon.
2. For Port Activation Options, choose a new script from the Script Name drop-down list.
3. Click Save to commit settings.

The system sends the request to the NetMRI appliance and displays a notification message.

The VLAN Reassignment task will also write the full running configuration to the device's memory, making it the saved configuration. If the user made a change to the running configuration, in parallel with the port activation change, and did not save it, those changes will also be saved.

Provision Bare Metal Device

The Provision Bare Metal Device automated task enables automated installation of new switches and routers into the network. The Trinzic Automation task enables cost and convenience savings by detecting the default behavior of new devices on the network, pointing them to customized TFTP servers from which standardized bare-metal configuration files are downloaded and installed onto the new devices.

The Provision Bare Metal Device automated task does not provide NIOS-based optional settings; configuration for this task is done in the Trinzic Automation 4000 NetMRI user interface. The automated task is automatically triggered by detection of a network device requiring configuration.

Rogue DHCP Server Remediation

All DHCP servers on the network should be under administrative control. If any device offering DHCP leases to clients on the network is not properly administered, it violates many security guidelines and at the very least may cause configuration problems throughout the network. Some events may be unwitting or innocuous (an office worker installing a wireless access point in their cube to share a resource), or may be an attempt to hijack clients and steal information. To prevent such issues, the Rogue DHCP Server Remediation task enables the detection, location and isolation of such devices.

The Provision Bare Metal Device automated task does not provide NIOS-based optional settings; configuration for this task is done in the Trinzic Automation 4000 NetMRI user interface. The automated task is automatically triggered by detection of a network device requiring remediation.

Using the Task Viewer to View Job Logs and Approve Jobs

You can view the logged results from any task run from the Automation Tasks dashboard through a pair of information pages, which are accessed through the Task Viewer window.

The Job History page provides a log history of all TAE tasks that have recently run, including all Automation Task types in the dashboard.

A second page, Issues & Approvals, provides links to two important items: Issues, which displays details about any network issue related to TAE tasks and jobs in an Issue Viewer page from the NetMRI appliance, and Approvals, which are jobs that must be approved before the NetMRI appliance can execute the job. For example, the Isolate Rogue DHCP Server job must be approved before it will run and attempt to isolate the detected rogue DHCP server in the network.

1. From the Dashboards tab, select the Tasks tab.
2. In the **Automation Tasks** pane, click the down arrow gadget and select **Task Viewer**. The Task Viewer window appears, displaying a scrollable and sortable Job History table. Important columns include the **Start Time**, the **Job ID** (a numeric value with a clickable link to the TAE Job Details Viewer, which will open in a new browser tab), the **Job Name**, the **User** account that executed the task, the **Job Status**, and the **# Devices** (the number of devices) against which the task ran. The Job History page shows the most recent subset of executed TAE jobs. A yellow bar at the top of the table provides a [click here to see more](#) link, which takes the user to the NetMRI appliance **Job History** page in a new browser tab.

3. If an item appears in the **Issues & Approvals** page, click the link in the **Action** column. You will typically see two different link types: **Issue Details** or **Approve Job**.
   a. To view an issue in more detail: Clicking an Issue Details link displays the NetMRI appliance Job Details page in a new browser tab for the selected job.
   b. To approve a job: Clicking an **Approve Job** link displays the **Summary** page of the NetMRI **Job Wizard**, with an **Approve Job** button.

4. Click **Close** to close the Task Viewer.

In the NetMRI appliance, you can also check **Configuration Management** → **Job Management** side tab → **Job History** and view details about any jobs that execute as a result of NIOS-based automation tasks.

### About Dashboard Templates

Superusers can specify the tasks an admin group can perform from the **Tasks Dashboard** tab by creating a dashboard template and assigning it to the admin group. When you create a dashboard template, you define the tasks users in an admin group can perform and specify whether the users can configure their own dashboards when they log in to Grid Manager. When you assign a dashboard template to an admin group, all users in this group can see and perform the tasks you define in the template, provided that the users also have the correct permissions to the objects related to the tasks. For information about administrative permissions, see [*Administrative Permissions for Dashboard Tasks*](#). If the assigned template is unlocked, users can configure tasks on their dashboard. If you lock the dashboard template, users cannot configure task packs on their own dashboards.

Superusers can also restrict limited-access users to access only the **Tasks Dashboard** tab when they log in to Grid Manager. These users cannot manage other core network services through Grid Manager. They can only see the **Tasks Dashboard** tab and access only the tasks defined in the dashboard template, if applicable. This feature is useful when you want to define different levels of admin users and restrict them to specific tasks based on their organizational functions. For information about how to set this restriction, see [*Creating Limited-Access Admin Groups*](#).

To configure and apply dashboard templates, complete the following:

1. Configure dashboard templates, as described in 4820090.
2. Assign dashboard templates to admin groups, as described in [*About Admin Groups*](#).

### Adding Dashboard Templates

Only superusers can configure dashboard templates. Limited-access users may configure task packs depending on the configuration of their assigned dashboard templates.

To add a dashboard template:

1. Log in as a superuser.
2. From the **Dashboards** → **Tasks** tab, click the Configure icon at the top right corner of a task pack.
3. Select tasks from the Active Tasks table and use the left arrow to move them to the Available Tasks table to hide the tasks, and vice versa. Grid Manager displays the tasks you place in the Active Tasks table. Repeat the steps for all task packs.
4. At the top right corner of the Tasks Dashboard panel, click the **Configure** icon → **Configure Template**.
5. In the Dashboard template configuration section, click **Create new template**.
6. In the **Save Dashboard Template** dialog box, complete the following:
   - **Name**: Enter a name for the new dashboard template.
   - **Locked**: When you select this check box and assign this template to an admin group, users in the admin group can only perform the tasks you configure to appear in this template. They cannot configure their dashboards. When you clear this check box, users can still only see the tasks you configure for this template, but they can now configure tasks in the task packs on their dashboards. Note that when you lock a template, it applies to all users in the admin group, including those who have customized dashboards.
7. Click **Save & Close**.

The appliance saves the template and adds it to the **Template** drop-down list.

### Resetting Dashboard Templates

Only users with an unlocked dashboard template assigned can reset their dashboards to the template that was originally assigned to them. Users with locked dashboard template cannot configure or reset their dashboards. Also, only superusers can configure dashboard templates.

To reset a dashboard template:

1. Select the **Dashboards** → **Tasks** tab.
2. For superusers: At the top right corner of the Tasks Dashboard panel, click the **Configure** icon → **Reset**. Note that the **Configure** icon appears only if you are a superuser.
   - For limited-access users: At the top right corner of the Tasks Dashboard panel, click **Reset**.

   The appliance reset your dashboard to the original dashboard template that was assigned to your admin group.
Modifying Dashboard Templates

You can modify an existing dashboard template by locking or unlocking it, and adding or removing tasks from a task pack. However, you cannot change the name of the template. When you change the name of a template, the appliance clones the template and adds the new template to the list. Note that when you modify a locked template that is assigned to an admin group, users in the group automatically adopt the changes you make to the template the next time they log in to Grid Manager.

To modify a dashboard template:

1. From the Dashboards -> Tasks tab, click the Configure icon at the top right corner of the panel.
2. In the Dashboard template section, select the template you want to modify from the Template drop-down list. Note that Grid Manager displays [L] before the name of a locked template.
3. In the task pack, click the Configure icon at the top right corner.
4. Select tasks from the Active Tasks tab and use the left arrow to move them to the Available Tasks table to hide the tasks, and vice versa. Grid Manager displays the tasks you place in the Active Tasks table. Repeat the steps for all task packs.
5. Click Save.
6. In the Save Dashboard Template dialog box, modify other information, as described in 4820090 4820090.
7. Click Save & Close.

Deleting Dashboard Templates

Only superusers can delete dashboard templates. To delete a dashboard template that is currently assigned to an admin group, you must first unassign the template from the admin group. For more information, see Creating Limited-Access Admin Groups.

To delete a dashboard template:

1. From the Dashboards -> Tasks tab, click the Configure icon at the top right corner of the panel.
2. In the Dashboard template section, select the template you want to delete from the Template drop-down list.
3. Click Delete.
4. In the Delete Dashboard Template dialog box, click Yes.

Assigning Dashboard Templates

After you create a dashboard template, you can assign it to an admin group. Admin users in this admin group can access the tasks you define in the template.

To assign a dashboard template to an admin group, see About Admin Groups.

Status Dashboards

A status dashboard contains widgets from which you can view and manage data. Widgets are the building blocks of status dashboards. For more information about widgets, see Adding Widgets to Dashboards. They provide information about different aspects of your Grid and networks. For example, the Member Status widget provides general information about a Grid member, and the Network Statistics widget provides data for a specified network.

The appliance provides a default status dashboard. Grid Manager displays the default dashboard only when there are more than one widget on the dashboard. You can add and modify widgets in the default dashboard, but you cannot rename or delete it. From a dashboard, you can access your most commonly accessed tasks and monitor appliance status. You can configure your own status dashboards to which you can add widgets that help you manage different data. Configuring multiple status dashboards helps organize widgets in a meaningful way and improves dashboard and widget performance. This is especially useful when you have a Grid serving a large number of Grid members. When you configure a new dashboard, you can use the existing dashboard as a template. You can create up to 100 copies at a time using the Add Dashboard option. For information about how to add status dashboards, see Adding Status Dashboards.

You can add widgets to different dashboards, however, you can add only one widget at a time on each dashboard. The default number of widgets per dashboard is 10. The maximum number of widgets that you can add on each dashboard is 20 at a time. You can define the number of widgets that can be configured on each dashboard in User Profile. This limitation applies only to dashboards that you configure and does not apply to the default dashboard. For information about how to specify the widget limit, see Configuring Widget Limit per Dashboard.

Grid Manager provides a default Security dashboard if you have installed any or all of the following licenses on the appliance: Threat Protection, RPZ, and Threat Analytics. The Security dashboard contains widgets that help you monitor the security status of the Grid. In the Security dashboard, you can add and remove widgets, but you cannot rename or delete them.

Note: To ensure that the Security dashboard displays correct data, use NTP to synchronize the time of the Grid members with that of the Grid Master.

If you have configured a lot of status dashboards, you can use the Quick Navigation icon to quickly access each status dashboard. For information, see Using Quick Navigation. Figure 2.1 illustrates the typical layout in Grid Manager after you configure multiple status dashboards.

Figure 2.1 Status Dashboard
You can do the following in the **Status** tab:

- Add new status dashboards, as described in Adding Status Dashboards
- Rename a dashboard, as described in Renaming Status Dashboards
- Copy or move a widget, as described in Copying or Moving Widgets
- Reorder dashboards, as described in Reordering Status Dashboards.
- Delete dashboards, as described in Deleting Status Dashboards.
- Configure widget limit, as described in Configuring Widget Limit per Dashboard.
- Configure Security dashboard properties, as described in Configuring Security Status Thresholds.

**Adding Widgets to Dashboards**

You can add all or some of the following widgets to your status dashboards depending on whether you are managing a Grid, an independent appliance, or an Infoblox Orchestration server:

- Grid Status
- Grid Upgrade Status
- Member Status (System Status)
- DNS Statistics
- Ranges Over Threshold
- IPv4 Failover Associations Status
- DHCP Statistics
- Network Statistics
- IPv4 Networks Over Threshold
- Discovery Status
- Advanced Discovery Status
- My Commands
- DDNS Statistics
- System Activity Monitor
- File Distribution Statistics
- Active WebUI Users
- Microsoft Servers Status Widget
- CSV Import Manager
- Load Balancer Status
- Pending Approvals
- Infoblox Community
- Infoblox Community
- Mobile Devices Status
Grid Manager displays the Security dashboard if you have any or all of the following licenses installed on your appliance: Threat Protection, RPZ, and Threat Analytics. The Security dashboard contains the following widgets, depending on the licenses installed on your appliance:

- Security Status for Grid
- Security Status for All Members
- Threat Protection Status for Grid
- Threat Protection Status for Member
- Response Policy Zone (RPZ) Status for Grid
- Response Policy Zone (RPZ) Status for Member

Note that you must have at least read-only permission to the objects that a widget displays. Otherwise, though you are allowed to select and place the widget on the dashboard, it does not display any information.

To add widgets to your dashboard:

1. **Default Status Dashboard**: From the Dashboards -> Status tab -> Default tab, click the Configure icon -> Add Content. This is applicable when you have the default dashboard only.

   **Configured Status Dashboards**: From the Dashboards -> Status tab, select the configured status dashboard, click the Configure icon -> Add Content.

2. **Security Status Dashboard**: From the Dashboards -> Status tab -> Security tab, click the Configure icon -> Add Content. This is applicable only when at least one member in the Grid has Threat Protection, RPZ, or Threat Analytics license. Note that the Security Status dashboard is a default dashboard and it cannot be renamed or deleted.

   Grid Manager displays thumbnails of the available widgets. Use the scroll bar on the right to scroll through the widgets, as illustrated in the Figure 2.2.

3. **Click an icon on the filter panel**, as illustrated in the Figure 2.2, to add a widget to the desired dashboard. Filter panel is categorized in to the following:
   - Cloud
   - Security
   - DNS/DHCP
   - and Reset

   When you click on an icon, Grid Manager displays thumbnails of the widgets belonging to the respective filter. If you click filters one after the other without clicking Reset, Grid Manager displays thumbnails of all widgets along with the icon that indicates the category to which the widget belongs. Click **Reset** to view only those widgets that belong to the selected category.

3. Select and drag a widget to the desired location on your dashboard. You can also click icon to add a widget to the desired dashboard.

   After you add a widget to the dashboard, you can configure it to provide relevant data. You can also copy or move a widget, by selecting and dragging it to its new location on your dashboard. Grid Manager saves your dashboard configuration and displays it the next time you log in.

   You can turn on auto-refresh by clicking **On** in the **Turn Auto Refresh** field at the top of the dashboard to periodically refresh the contents of all widgets in the dashboard. Click **Off** to disable auto-refresh for all widgets in the dashboard. When auto-refresh is disabled, you can enable it for individual widgets by clicking the Configure icon in the corresponding widgets. You can specify the auto-refresh period in seconds. The default auto-refresh period is 30 seconds.

   Widgets have the following icons:

   - **Copy/Move**: Click to copy or move the widget from a dashboard to another. For information about how to copy or move, see **Copying or Moving Widgets**.
   - **Span Up/Span Down**: Click to resize the widget. Click **Span Up** to increase the width of the widget. Click **Span Down** to decrease the width of the widget. Note that the fully spanned widgets are moved to the top of the dashboard.
   - **Refresh**: Click to update the content of the widget. Each widget contains a status bar at the bottom that displays the last date and time it was updated.
   - **Configure**: Click to hide and show the configuration options of the widget.
   - **Toggle**: Click to minimize and restore the widget.
   - **Close**: Click to remove the widget from a dashboard.

---

Figure 2.2 Widgets Panel
Configuring Widget Limit per Dashboard

You can define the number of widgets that can be configured on each dashboard. This limitation applies only to dashboards that you configure and does not apply to the default dashboard.

1. From the **Dashboards** -> **Status** tab, click the Configure icon -> **User Profile**.
2. In the **User Profile** editor, complete the following:
   - **Maximum Widgets per Dashboard**: Specify the maximum number of widgets that can be configured per Dashboard. You can enter a value between 1 and 20. The default value is 10. This limit does not apply to the default dashboard.
3. Save the configuration and click **Restart** if it appears at the top of the screen.

Adding Status Dashboards

You can create your own status dashboards and add the widgets that you need. You can configure up to 100 status dashboards at a time. When you create multiple instances of a dashboard, the appliance names each dashboard by adding an incremental suffix to the name of the new dashboard. For example, if you name a new dashboard "Corp_Dashboard" and specify the number of instances as three, then the appliance creates three instances of this new dashboard. In this example, the appliance creates three dashboards: Corp_Dashboard, Corp_Dashboard1, and Corp_Dashboard2. Note that the dashboards you create will not be available to other users. You cannot share dashboards you have created with other users.

Note that "Security" is reserved for the default Security dashboard. Grid Manager displays an error message if you name a new dashboard "Security".

To add a new status dashboard:

1. From the **Dashboards** -> **Status** tab, click the Configure icon -> **Add Dashboard**.
2. In the **Add Dashboard** wizard, complete the following:
   - **Name**: Enter a name for the new dashboard.
   - **Add <= instances of this new dashboard**: Enter the number of dashboards you want to create. The maximum number of dashboards you can create is 100 at a time.
   - **Copy initial content from an existing dashboard**: Select this check box if you want the appliance to copy the contents from an existing status dashboard into the new dashboard. After you select this check box, the appliance displays the list of configured dashboards. Select a dashboard from the list. By default, this check box is not selected.
3. Save the configuration.

The appliance displays all dashboard instances in the **Status** tab.

Using Quick Navigation
You can use the Quick Navigation icon to quickly access a specific dashboard. The appliance provides the Quick Navigation icon at the right corner of the status dashboards, as illustrated in Figure 2.1.

To quickly navigate to a dashboard:

1. From the **Dashboards** -> **Status** tab, click the Quick Navigation icon at the right corner of the dashboards. The list of configured dashboards are displayed.
2. Select a dashboard or specify the name of the dashboard in the text box. The appliance displays the selected dashboard.

### Renaming Status Dashboards

You can rename only the status dashboards that you have configured. You cannot rename the default dashboard and the Security dashboard.

To rename a dashboard:

1. From the **Dashboards** -> **Status** tab, click the Configure icon -> **Rename Dashboard**.
2. In the **Rename Dashboard** wizard, complete the following:
   - **Select a dashboard**: Select a dashboard from the drop-down list.
   - **Name**: Enter the new name of the dashboard.
3. Do one of the following:
   - **Click Save and Close** to save the new name and close the wizard.
   - **Click Save** to save the new name and continue to rename other dashboards.

To rename a specific dashboard:

1. From the **Dashboards** -> **Status** tab, select a dashboard that you want to rename.
2. Click the Configure icon -> **Rename Dashboard**.
3. In the **Rename Dashboard** wizard, enter the new name in the **Name** text box.
4. Click **Save and Close** to save the new name and close the wizard.

### Copying or Moving Widgets

You can copy or move a widget from one dashboard to another. When you add a widget that already exists, the appliance displays an error message. When you move a widget, it is moved from the source to the destination dashboard. The moved widget will not be available in the source dashboard any more. When you copy a widget, the widget is duplicated and is available in both the source and destination dashboards. Note that the Copy/Move icon is not available in a widget if the appliance has only the default status dashboard.

To move or copy a widget:

1. From the **Dashboards** -> **Status** tab, select a status dashboard.
2. Select the widget that you want to copy or move, and then click the Copy/Move icon.
3. In the **Copy/Move <name of the widget>** wizard, complete the following:
   - **Copy**: Select this to copy a widget.
   - **Move**: Select this to move a widget.
   - **To Dashboard**: Select the name of the destination dashboard.
4. Click **OK**.

### Reordering Status Dashboards

You can change the order of your status dashboards. When you add a new status dashboard, it is added as a tab. When you create multiple instances of a dashboard, they are added as subsequent tabs. You can arrange the order of each dashboard through the reordering process.

To reorder status dashboards:

1. From the **Dashboards** -> **Status** tab, click the Configure icon -> **Reorder Dashboards**.
2. The following are displayed in the **Order Dashboards** wizard:
   - **Ordering**: You can use the up and down arrows to move dashboards in the desired order or drag and drop them to the desired positions.
   - **Dashboard**: Displays the list of all the status dashboards.
3. Click **OK** to save the changes.

### Deleting Status Dashboards

You can delete status dashboards that you have configured. You cannot delete the default status dashboard and the Security dashboard. You can delete multiple dashboards at the same time. Note that you cannot restore a deleted dashboard.

To delete multiple dashboards:

1. From the **Dashboards** -> **Status** tab, click the Configure icon -> **Delete Dashboards**.
2. In the **Delete Dashboards** wizard, select the **Dashboard** check box. You can select multiple check boxes for multiple dashboards.
3. Click Delete.
4. Click Yes in the confirmation dialog box. To delete a specific dashboard:
5. From the Dashboards -> Status tab -> select the <Status Dashboard> tab.
6. Click the Configure icon -> Delete Dashboard.
7. In the Delete Confirmation dialog box, click Yes.

### Configuring Security Status Thresholds

You can configure thresholds to determine the overall status of Threat Protection, DNS RPZ (Response Policy Zone), and DNS Threat Analytics services in the Grid. Grid Manager provides a view of the overall security status of the Grid in the Security Status for Grid dashboard widget. For information, see Security Status for Grid.

To configure the thresholds for security status:

1. From the Dashboards -> Status tab, click the Configure icon -> Global Dashboard Properties.
2. In the Global Dashboard Properties editor, complete the following:

   - **Threat Protection Thresholds**: Define the thresholds for each severity level of the threat protection events for the following colors:
     - Yellow: Specify the low threshold value for Critical, Major, and Warning severity level. The default values are 1, 20, and 100 for Critical, Major, and Warning respectively.
     - Red: Specify the high threshold value for Critical, Major, and Warning severity level. The default values are 5, 100, and 1000 for Critical, Major, and Warning respectively.

   Depending on the specified thresholds, Grid Manager determines the status of threat protection service as follows, which is displayed in the Status column of the Security Status for Grid widget:

     - Green (OK): When the number of threat protection events are less than the low threshold value specified for the yellow color for all the severity levels.
     - Yellow (Warning): When the number of threat protection events equals or exceeds the threshold value specified for the yellow color but less than the threshold value specified for the red color for any of the severity levels.
     - Red (Critical): When the number of threat protection events equals or exceeds the high threshold value specified for the red color for any of the severity levels.

   - **Response Policy Zone Thresholds**: Define the threshold values for the following colors to determine the overall status of RPZ:
     - Yellow: Specify the low threshold value for Blocked, Substitute, and Passthru RPZ rules. The default values are 10, 1, and 100 for Blocked, Substitute, and Passthru respectively.
     - Red: Specify the high threshold value for Blocked, Substitute, and Passthru RPZ rules. The default values are 100, 10, and 1000 for Blocked, Substitute, and Passthru respectively.

   Depending on the specified thresholds, Grid Manager determines the status of RPZ as follows, which is displayed in the Status column of the Grid Security Status widget:

     - Green (OK): When the number of RPZ hits are less than the low threshold value specified for the yellow color for all the rule types.
     - Yellow (Warning): When the number of RPZ hits equals or exceeds the threshold value specified for the yellow color but less than the threshold value specified for the red color for any of the rule types.
     - Red (Critical): When the number of RPZ hits equals or exceeds the high threshold value specified for the red color for any of the rule types.

   - **Threat Analytics Thresholds**: Define the thresholds for the following colors, to determine the overall status of DNS Threat Analytics:
     - Yellow: Specify the low threshold value for DNS Tunneling events. The default value is 1.
     - Red: Specify the high threshold value for DNS Tunneling events. The default value is 5.

   Depending on the specified thresholds, Grid Manager determines the status of DNS Threat Analytics as follows, which is displayed in the Status column of the Grid Security Status widget:

     - Green (OK): When the number of DNS tunneling attacks are less than the low threshold value specified for the yellow color.
     - Yellow (Warning): When the number of DNS tunneling attacks equals or exceeds the threshold value specified for the yellow color but less than the threshold value specified for the red color.
     - Red (Critical): When the number of DNS tunneling attacks equals or exceeds the high threshold value specified for the red color.

3. Save the configuration.

### Grid Status

The Grid Status widget provides status information about the Grid members and services. Add the Grid Status widget to your Dashboard to monitor the Grid status.

You can configure the Grid Status widget to display information about all Grid members or only Grid members that have service errors. To modify the Grid Status widget, click the Configure icon and select one of the following:

---

**Note:** If you have configured the same threshold value for both Yellow and Red color in the Global Dashboard Properties editor and if the same number of events are triggered, then Grid Manager displays the status in red in the Grid Security Status widget.
- **Show all Grid members** (this is the default)
- **Only show members with service warnings or errors**: When you select Only show members with service warnings or errors, the widget displays only the members that have service errors. The widget does not display any data in the member table if all the services on all members are running properly.
- **Group Members by**: If you want to group members by the same extensible attribute value, select this and choose an extensible attribute from the drop-down list. The appliance groups Grid members that have the same extensible attribute value, and the Grid Status displays the following information:
  - `<Extensible Attribute Name>`: The value of the selected extensible attribute. You can click the link of the extensible attribute value to view all the members in this group in the Grid/Members view.
  - **Status**: This is the overall status for all members in the group. Depending on the status of each member, the overall status can be one of the following:
    - **Working**: Indicates that all the members in the group are running properly.
    - **Warning**: Indicates that one of the member in the group has operational problems. For example, if there are two members in a group with one member Running and another member is Offline, then the overall status will be Warning.
    - **Failed**: Indicates that at least one of the members in the group is in the failed status and none of the members in the group are in the Running or Working status. For example, if there are two members in the group and one of them is in Failed status and the other is Offline, then the overall status is Failed.
    - **Offline**: Indicates that one or more members in the group is offline and none of the members in the group are in the Failed or Running status. For example, if a member is in the Working status and another member is in the Offline status, then overall status is Offline.
    - **Inactive**: Indicates that one or more members in the group is inactive and none of the members in the group are in the Failed, Offline, Working, or Running status.
    - **Unknown**: Indicates that the status of all the members in the group is unknown.

**Note**: You can click a member link to monitor the detailed status of the selected member. Grid Manager displays the Grid tab -> Member tab. For information, see Member Status. You can click on a group to show the members of the group in the Grid/Members view.

The **Grid Status** widget also displays the following information in the member table:

- **Member Name**: The name of the member.
- **IPv4 Address**: The IPv4 address of the member.
- **IPv6 Address**: The IPv6 address of the member.
- **Status**: The current status of the member.
- **System Uptime**: The duration of time (days, hours, and minutes) that the Grid member has been up and running.

In the upper section of the widget, Grid Manager displays the overall status of the Grid. The Grid status represents the status of the most critical member in the Grid. When all Grid members are running properly, the overall Grid status is green. When one of the members has operational issues, the overall Grid status is red. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>All Grid members are operating normally in a “Running” state.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>At least one of the Grid members is connecting or synchronizing with its Grid Master.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>At least one of the Grid members does not have a Grid license, is offline, upgrading, downgrading, or shutting down.</td>
</tr>
</tbody>
</table>

This section also displays the overall operational status of the DNS, DHCP, NTP, FTP, TFTP, HTTP (File Distribution), bloxTools, Captive Portal, DNS Accelerator usage, and Reporting services that are currently running on the Grid. The DNS Accelerator usage feature is only available in the IB-4030 appliance. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green" /></td>
<td>Green</td>
<td>The enabled service is running properly on one or more Grid members.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow" /></td>
<td>Yellow</td>
<td>At least one of the Grid members is having issues with the enabled service.</td>
</tr>
<tr>
<td><img src="image" alt="Red" /></td>
<td>Red</td>
<td>The enabled service is not running properly on at least one of the members. (A red status icon can also appear temporarily when the service is enabled and begins running, but the monitoring mechanism has not yet notified Grid Manager.)</td>
</tr>
</tbody>
</table>
Grid Upgrade Status

The Grid Upgrade Status widget provides upgrade status of the Grid Master and members. Add the Grid Upgrade Status widget to your Dashboard to monitor the upgrade status of the Grid and its members.

The Grid Upgrade Status widget displays the following information:

- **Upgrade Status**: The current upgrade status of the Grid. This can be Running, Paused, Canceled, or Inactive.
- **Grid Member Upgrade Process Status**: The pie chart shows the number of members that are still processing the upgrade, members that have completed the upgrade, and members that are waiting for the upgrade to happen.
- **Detailed Upgrade Status**: Click this link to access the Grid tab -> Upgrade tab to see detailed information about the upgrade.

The table on the right shows a summary of the upgrade status of the upgrade groups. It displays the following information:

- **Group**: The name of the upgrade group.
- **Date/Time**: The date and time when the upgrade started on this upgrade group. Note that the time zone is the time zone of the first member in the upgrade group.
- **Completed**: Indicates whether the upgrade is complete or not.

Member Status (System Status)

The Member Status widget provides status information about the system resources and services of a Grid member, including the reporting server. Add a Member Status widget to your Dashboard for each Grid member that you want to monitor. The widget always displays the services that a Grid member is running. You can then configure it to display additional information and specify how the information is displayed.

You can modify the Member Status or the System Status widget by clicking the Configure icon. If you have an independent appliance, you can only configure some of the following:

- For Member Status widget only: Click Select Member to select a Grid member for display. When you select the reporting server, the widget displays reporting usage.
- Select the information you want to display:
  - **Show Role**: For Member Status widget only. Click to display whether the appliance is a Grid Master, Grid Master candidate, or Grid member. An independent appliance does not have a Grid license installed.
  - **Show Hardware Type**: Click to display the appliance hardware model.
  - **Show HA Status**: Click to display whether the appliance is part of an HA pair. It displays one of the following:
    - **HA OK**: The Grid member is part of an HA pair that is functioning properly.
    - **HA Broken**: The appliance is part of an HA pair that is not operating properly. You can check the logs to determine the problem.
  - **Show System Uptime**: Click to display the duration of time (days, hours, and minutes) that the Grid member has been up and running.
  - **Statistics**: Select the data that you want to display and its format:
    - **CPU**: Click to display the percentage of CPU that is in use. Select either Dial or Bar for the display format.
    - **Memory**: Click to display the current percentage of memory that is in use. Select either Dial or Bar for the display format.
    - **Database**: Click to display the percentage of the database that is in use. Select either Pie or Bar for the display format.
    - **Disk**: Click to display the percentage of the data partition on the hard disk drive in use. Select either Pie or Bar for the display format.
    - **System Temperature**: Click to display the system temperature. Depending on the hardware model, the system temperature may not be available. Select to display the temperature in either Celsius or Fahrenheit.
    - **CPU Temperature**: Click to display the CPU temperature. Depending on the hardware model, the CPU temperature may not be available. Select to display the temperature in either Celsius or Fahrenheit.
    - **DNS Accelerator Usage**: This feature is only available in the IB-4030 appliance. Click to display the percentage of DNS Cache Acceleration usage, if available. When the DNS cache acceleration utilization reaches the maximum threshold, the appliance displays both the Member Status and the banner in yellow each time you log in to the appliance within 24 hours. It also displays the number of times the appliance has reached the maximum limit in the past 24 hours. For example, if you are using a DNS Cache Acceleration Tier 3 license with 300K performance, and if the DNS Cache Acceleration usage has reached 250K, then the appliance displays the DNS Cache Acceleration usage as 83%, which is calculated as (250/300)/300. In this case, the appliance displays the following message in the banner:
      DNS Cache accelerator usage reached 83% of the maximum capacity 6 times in the last 24 hours.

Click the Configuration icon again to hide the configuration panel after you complete the modification.

Grid Manager displays the hostname of the appliance at the top of the widget. You can click the name link to view detailed information about the appliance. The widget also displays the upgrade status if the member is currently in the process of an upgrade. If the member is scheduled for an upgrade, the Scheduled for upgrade link appears. You can click this link to access the Grid tab -> Upgrade tab to view more details about the date and time of the scheduled upgrade.
The widget also displays the service status of the following: FTP, TFTP, HTTP (File Distribution), DNS, DHCP, NTP, bloxTools, Captive Portal, DNS Accelerator, and Reporting in the Services section. The service status can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green Icon]</td>
<td>Green</td>
<td>The service is enabled and running properly.</td>
</tr>
<tr>
<td>![Yellow Icon]</td>
<td>Yellow</td>
<td>The service is enabled, but there may be some issues that require attention.</td>
</tr>
<tr>
<td>![Red Icon]</td>
<td>Red</td>
<td>The service is enabled, but it is not running properly or is out of synchronization. (A red status icon can also appear temporarily when a service is enabled and begins running, but the monitoring mechanism has not yet notified the GUI engine.)</td>
</tr>
<tr>
<td>![Gray Icon]</td>
<td>Gray</td>
<td>The service is not configured or is disabled.</td>
</tr>
</tbody>
</table>

The widget also displays the statistics you specified, such as CPU usage, memory and database usage, in the format you selected. When you select the reporting server, you can also see the reporting usage information:

- **Reporting Usage**: Displays the daily consumption rate for the reporting service.

For more information about reporting, see [Infoblox Reporting and Analytics](#).

**DNS Statistics**

The DNS Statistics widget provides statistics for a member or for a zone. The zone statistics are cumulative, collected from all the members that are authoritative servers for zones or are hosting stub zones. The widget displays the totals for each type of DNS response as well as a line graph that tracks the responses per second.

You can add a DNS Statistics widget to your Dashboard for each zone or member DNS server on the Grid. To configure the DNS Statistics widget, click the Configure icon and do the following:

- Click **Select Member**. In the Member Selector dialog box, choose a Grid member to display statistics for all its stub zones and authoritative zones.

  or

- Click **Select Zone**. In the Zone Selector dialog box, choose a DNS zone to display statistics for that zone only.

The widget displays only the option that you selected on your subsequent logins. For example, if you clicked **Select Member**, the widget displays the Select Member option only, and not the Select Zone option, when you log in again.

- **Graph Configuration**: Select which DNS messages you want to track in the Responses per Second graph.
  - **Success**: The number of successful queries.
  - **NXDOMAIN**: The number of queries for domain names that did not exist in the database.
  - **Referral**: The number of queries that became referrals.
  - **NXRRSET**: The number of queries for domain names that did not have the requested records.
  - **Failure**: The number of queries that failed due to reasons other than nonexistent domain names or records in a domain.
  - **Recursion**: The number of recursive queries for which the name server sent queries to other name servers.

The widget displays the following information:

- **DNS Responses** tab: Displays a pie chart and the total number of each type of message. It also displays the total number of full and incremental zone transfers that the Grid member performed.

- **Responses per Second** tab: Displays a line graph that tracks the DNS responses received per second, within an hour. The time is displayed according to the time zone specified in the User Profile. If the auto-detect time zone option is enabled and Grid Manager cannot determine the browser time zone, then the time is displayed in UTC format. You can mouse over the graph to display the coordinates of any point in the graph.

**Ranges Over Threshold**

The Ranges Over Threshold widget enables you to monitor IPv4 DHCP range usage from your Dashboard. It lists the IPv4 ranges that are allocated above a specified threshold and thus may warrant your attention. The default threshold is 75%. For information, see [Configuring Thresholds for DHCP Ranges](#). Note that the appliance highlights disabled IPv4 ranges in gray.

The widget displays the IPv4 ranges with utilization percentages that surpass the threshold. To configure the Ranges Over Threshold widget, click the Configure icon and do the following:
 IPv4 Failover Associations Status

The IPv4 Failover Associations Status widget enables you to monitor the status of the failover associations from your Dashboard. It lists all the failover associations in the Grid and displays their names and status. The widget also displays the primary and secondary servers in the association. When you click a failover association link or a status link, Grid Manager displays the Failover Association section where you can get detailed information about the failover association. For information, see Monitoring Failover Associations.

To configure the IPv4 Failover Associations widget, click the Configure icon and do the following:

- Click the Export button to export the list of IPv4 ranges that surpass the threshold to a file in CSV format.
- Click the Refresh button to refresh the data in the list.

DHCP Statistics

The DHCP Statistics widget displays statistics about the different types of DHCP messages that a Grid member sends and receives. The widget displays the totals for each type of DHCP message as well as a line graph that tracks the messages per second.

You can add a DHCP Statistics widget to your Dashboard for each member DHCP server in the Grid. If the DHCP service is not enabled or is offline, the widget displays a message indicating that the DHCP statistic are not available.

To configure the DHCP Statistics widget, click the Configure icon and do the following:

- **Protocol**: Select either IPv4 or IPv6.
- Click **Select Member**. In the Member Selector dialog box, select a Grid member from the list.
- **Graph Configuration**: This section lists IPv4 or IPv6 messages, depending on the protocol you selected.
- Select which IPv4 messages you want to track in the Messages per Second graph.
  - **Discovers**: The number of DHCPDISCOVER messages that the Grid member received from DHCP clients. A DHCP client broadcasts a DHCPDISCOVER message to obtain an IP address.
  - **Offers**: The number of DHCPOFFER messages that the Grid member sent to DHCP clients. If the Grid member has an IP address that it can allocate to the DHCP client that sent the DHCPDISCOVER message, the Grid member responds with a DHCPOFFER message that includes the IP address and configuration information.
  - **Requests**: The number of DHCPREQUEST messages that the Grid member received from DHCP clients. A DHCP client sends DHCPREQUEST messages when it selects a lease, connects to the network, and if it renews the lease.
  - **Acks**: The number of DHCPACK messages that the Grid member sent to DHCP clients. When the Grid member receives a DHCPREQUEST message, it responds with a DHCPACK message to confirm the IP address selected by the DHCP client.
  - **Nacks**: The number of DHCPNACK messages that the Grid member sent to DHCP clients. The Grid member sends a DHCPNACK message when a DHCP client requests an IP address that is not valid for the network.
  - **Declines**: The number of DHCPDECLINE messages that the Grid member received. A DHCP client sends a DHCPDECLINE message to a DHCP server when it discovers that the IP address offered by a DHCP server is already in use.
  - **Informs**: The number of DHCPINFORM messages that the Grid member received. A client that did not receive its IP address from the DHCP server can send it a DHCPINFORM message to retrieve configuration parameters, such as the IP addresses of DNS servers in the network.
  - **Releases**: The number of DHCPRELEASE messages that the Grid member received. A DHCP client sends a DHCPRELEASE message when it terminates its lease and releases its IP address.

Select which IPv6 messages you want to track in the Messages per Second graph.

- **Declines**: The number of Decline messages that the Grid member received. A DHCP client sends a Decline message to a DHCP server when it discovers that the IP address offered by a DHCP server is already in use.
- **Renews**: The number of Renew messages that the Grid member received. A DHCP client sends a Renew message to a DHCP server to extend the lifetimes on the leases granted by the DHCP server and to update other properties.
- **Information Requests**: The number of Information-Request messages that the Grid member received. A client sends an Information-Request message to retrieve configuration parameters, such as the IP addresses of DNS servers in the network.
- **Solicits**: The number of Solicit messages that the Grid member received, including Solicit messages embedded in Relay-Forward messages. A DHCP client sends a Solicit message to locate DHCP servers.
- **Requests**: The number of Request messages that the Grid member received. A DHCP client sends a Request message to request one or more IP addresses and configuration parameters from a DHCP server.
- **Rebinds**: The number of Rebind messages that the Grid member received. A DHCP client sends a Rebind message to extend the lifetime of its lease and to update configuration parameters.
- **Releases**: The number of Release messages that the Grid member received. A DHCP client sends a Release message when it terminates its lease and releases its IP address.
- **Advertisements**: The number of Advertise messages that the Grid member sent. When a DHCP server receives a Solicit message, it can respond with an Advertise message to indicate that the server is available for DHCP service.
- **Replies**: The number of Reply messages that the Grid member sent. A DHCP server sends a Reply message that includes IP
addresses and configuration parameters when it responds to Solicit, Request, Renew or Rebind message. It sends a Reply message with configuration parameters only when it responds to an Information-Request message.

The widget displays the following information:

- **DHCP Messages** tab: Displays a pie chart and the totals for each type of DHCP message. It also displays the number of Deferred Updates, which are DDNS update requests which are deferred because the DNS primary was not reachable when the update was first attempted.

- **Messages per Second** tab: Displays a line graph that tracks the DHCP messages that were sent and received per second, within an hour. The time is displayed according to the time zone specified in the User Profile. If the auto-detect time zone option is enabled and Grid Manager cannot determine the browser time zone, then the time is displayed in UTC format. You can mouse over the graph to display the coordinates of any point in the graph.

### Network Statistics

The **Network Statistics** widget provides information about IP address usage in an IPv4 network. You can monitor several networks simultaneously to view the distribution of address resources. Such information can indicate if there is a sufficient number of available addresses in each network. It can also provide information about the distribution of address resources, indicating if there are too many unused addresses in one network while all the addresses in another are in use.

**Add a Network Statistics widget to your Dashboard for each network that you want to monitor.** You can monitor IPv4 networks only.

To configure the **Network Statistics** widget, click the Configure icon and do the following:

- Select one of the following chart types:
  - Pie
  - Bar

- Click **Select Network**. In the **Network Selector** dialog box, choose a network from the list and click **Select**.

  Note that if multiple network views were previously configured, Grid Manager displays the default network view. You can choose another network view from the drop-down list, and then select a network.

  The **Network Statistics** widget displays the following information about the selected network:

  - **IPAM Utilization**: When you define a network, this is the percentage based on the IP addresses in use divided by the total addresses in the network. For example, in a /24 network, if there are 25 static IP addresses defined and a DHCP range that includes 100 addresses, the total number of IP addresses in use is 125. Of the possible 256 addresses in the network, the IPAM utilization is about 50% for this network.

  When you define a network container that contains subnets, this is the percentage of the total address space defined within the container regardless of whether any of the IP addresses in the subnets are in use. For example, when you define a /16 network and then 64 /24 networks underneath it, the /16 network container is considered 25% utilized even when none of the IP addresses in the /24 networks is in use.

  You can use this information to verify if there is a sufficient number of available addresses in a network. The IPAM utilization is calculated approximately every 15 minutes.

- **Unmanaged**: The number of discovered IP addresses that do not have corresponding records on the appliance, such as A records, PTR records, fixed address records, host records, or leases. To obtain this data, you must run a discovery process on the network first.

- **Conflicts**: The number of IP addresses that have either a MAC address conflict or a DHCP range conflict. To obtain this data, you must run a discovery process on the network first. A discovered host has a MAC address conflict when its MAC address is different from that specified in its fixed address, DHCP lease, or host record. A discovered host has a DHCP range conflict when it is part of a DHCP range, but it does not have a matching fixed address or DHCP lease, and it is not part of an exclusion range.

### Network Users - Active Users

The **Network Users Active Users** widget displays up to 10 active users for Windows devices managed by the Grid. To modify the **Network Users Active Users** widget, click the Configure icon and select one of the following:

- **Only show networks with**: Select **At least** or **Fewer than** from the drop-down list and specify the number of users in the **Users** field. The default values are set to **At least** and **10** users.

- **All Network Views**: Select this to monitor active users on the managed Active Directory domains in all network views.

- **Select Network View**: Click **Select** to select the network view in which you want to monitor active users.

  The **Network Users-Active Users** widget displays the following information:

  - **Network**: The network address. You can click the network link to view network details.

  - **Active Users**: All users who are currently using the Active Directory domains. You can also export the list to a .csv file.

### IPv4 Networks Over Threshold

The **IPv4 Networks Over Threshold** widget enables you to monitor IPv4 network and IP address usage from your Dashboard. It lists the IPv4 networks that are allocated above a specified threshold and thus might warrant your attention. The default threshold is 75%.

For network containers, the threshold is the percentage of IP address space that has been allocated. For subnets, it is the percentage of used addresses, except the broadcast and network addresses. The widget displays the network containers and subnets with utilization percentages that surpass the threshold.

You can also select to view IPv4 cloud networks only if you have deployed Cloud Network Automation. For information about this feature, see *Deploying Cloud Network Automation*.

To configure the **Networks Over Threshold** widget, click the Configure icon, and then complete the following:
- **Threshold**: Enter a new threshold value. The default is 75%.
- **Type**: Select IPAM Utilization or IPv4 DHCP Utilization. For information, see Managing IPv4 DHCP Data.
- **All Network Views**: Select this to monitor threshold for IPv4 networks in all network views.
- **Select Network View**: Click Select to select the network view in which you want to monitor the threshold.

To view information related to cloud networks, select **View Cloud Networks Only**, and then select one of the following:

- **All Tenants**: Displays information for all tenants.
- **Select Tenant**: Click Select to select a specific tenant. In addition, you can do the following in this widget:
  - Click the Export button to export the list of networks that surpass the threshold to a file in CSV format.
  - Click the Refresh button to refresh the data in the list.

### Port Status

The Port Status widget provides a quick way to inspect the interface status for any discovered device in the network. The widget shows an overview of all interfaces on all devices or for a single device (called the Data Scope).

Click the Configure icon to change settings for the widget.

1. You can choose a **Bar** or **Pie** chart for the **Total Switch or Switch-Router** chart, which shows the percentage of ports that are operationally Active and that are operationally Down.
2. Under **Data Scope**, the **All Devices** setting allows the widget to show the total counts for all discovered network infrastructure devices. This is the default.
3. To use the widget to display port information for a single device, such as a switch, enable the **Select Device** radio button. Choose the device in the **Device Selector** window. The widget adjusts its reported values to the scale of the selected device.
4. You can also choose the **Media Type** to further filter port status information. Choices include: Ethernet Interface, Layer 2 Virtual LAN, Proprietary Serial Interface, Proprietary Virtual/Internal Interface, Loopback Interface and Tunnel Interface.

The counters in the widget include **Total Switch and Switch-Router Ports**, **Total Down Switch and Switch-Router Ports** and **Total Active Switch and Switch-Router Ports**.

### Discovery Status

The appliance can run an IP discovery to detect and obtain information about active hosts in specified networks. For information about the discovery process, see [IP Discovery and vDiscovery](#).

You can add the **Discovery Status** widget to your Dashboard. From this widget, you can access Discovery Manager and configure parameters for a discovery. You can do the following from the widget:

- Start a discovery immediately. For more information about immediate discovery, see Configuring and Starting an IP discovery.
- Schedule a discovery for a later date and time. For more information about discovery, see Scheduling IP Discovery.
- Configure a recurring discovery. For more information about recurring discovery, see Scheduling IP Discovery.
- Click the Start button to start a discovery process.
- Click the Pause button to temporarily pause the process.
- Click the Stop button to stop the process.

This widget displays the status of discovery tasks. If there are no active discovery tasks, the widget displays the discovery results of the previous tasks. For information about starting and scheduling a discovery task, see Guidelines for Starting and Scheduling IP Discovery.

After you start a discovery, the **Discovery Status** widget displays a status bar that indicates the discovery is in progress. It also tracks the number of networks in an IP discovery. You can click the Refresh icon to update the discovery status.

The widget displays the following information about the discovery process:

- **Current Status**: If a discovery is in progress, this field displays its current status. Otherwise, it displays the date and time of the last discovery.
- **Last Action**: Displays the last operation and the admin who initiated it.
- **IPv4 Device Discovery**: Displays the total number of IPv4 networks and the IPv4 network and IP address range on which the IP discovery is currently running. You can click Refresh to update this information.

The **Discovery Status** widget also displays the following information about the last discovery:

- **Discovered**: The total number of active hosts in the network.
- **Managed**: The number of discovered IP addresses that are managed by the NIOS appliance. These IP addresses have an A record, PTR record, fixed address record, host record, lease, or are within a configured DHCP range.
- **Unmanaged**: The number of discovered IP addresses that do not have corresponding records on the appliance, such as A records, PTR records, fixed address records, host records, or leases.
- **Conflicts**: The number of discovered hosts that have a MAC address conflict or are part of a configured DHCP range, but do not have a fixed address or lease record and are not part of an exclusion range.

### Advanced Discovery Status
With the correct licensing, dedicated NIOS appliances operating as Grid members can perform infrastructure device discovery. NIOS appliances with the Discovery license operate primarily for discovery tasks and do not perform core DNS or DHCP network functions. Discovery appliances, called Probes, collect all network device data and compile it into a database. A separate NIOS appliance, called a Consolidator, aggregates the collected device information from the Probes and synchronizes with the Infoblox Grid Master.

For more information about discovery and its features and requirements, see the chapter *Infoblox Network Insight* and its associated sections. The Advanced Discovery Status widget provides several basic counts describing the general state of device discovery within the Grid, and for networks outside the Grid being inventoried by the NIOS appliances designated for discovery. The widget divides counters into two categories: **Networks** and **Assets**. Network counters refer to counts of managed and unmanaged networks discovered by Probe appliances. Asset counters refer to counts of specific types of network devices, termed Assets, which are comprised of end hosts, enterprise servers, enterprise printers, and any other enterprise asset that exists in an end-user network segment. The widget counters include:

- **Networks category:**
  - **Discovered:** The total number of networks discovered by Probe appliances.
  - **Managed:** The number of discovered networks that are currently managed by the NIOS Grid. These IP networks have been converted from Unmanaged status to Managed status.
  - **Unmanaged:** The number of discovered networks that are counted as Unmanaged by the NIOS Grid Master. After a network is discovered and catalogued by a Probe appliance, its default state as a network is Unmanaged.

- **Assets category:**
  - **Discovered:** The total number of Assets discovered by Probe appliances.
  - **Managed:** The number of discovered assets that are currently managed by the NIOS Grid. These devices have been converted from Unmanaged status to Managed status.
  - **Unmanaged:** The number of IPs with discovered data that are counted as Unmanaged by the NIOS Grid Master, and have not been converted into a Host or a Fixed IP Address. After an Asset is discovered and catalogued by a Probe appliance, its default state is Unmanaged.
  - **Conflicts:** The number of discovered assets that have a MAC address conflict or are part of a configured DHCP range, but do not have a fixed address or lease record and are not part of an exclusion range.

**My Commands**

The *My Commands* widget provides easy access to commands that you frequently use, so you can perform your tasks without leaving the Dashboard. You can add one *My Commands* widget to your Dashboard.

To configure the *My Commands* widget, click the Configure icon and do the following:

- Select a command from the **Available** list and click the > arrow to move it to the **Selected** list. You can always toggle the commands between the two lists. Select multiple commands by using SHIFT-click and CTRL-click.

**DDNS Statistics**

The *DDNS Statistics* widget provides information about the dynamic DNS (DDNS) updates that occur on the DNS service of a selected Grid member. The widget displays the total number of DDNS updates that succeeded, failed, and that were rejected. It also displays a line graph that tracks the status of the DDNS updates per second.

You can add a *DDNS Statistics* widget to your Dashboard for each DNS server on the Grid that accepts dynamic DNS updates.

To configure the *DDNS Statistics* widget, click the Configure icon and do the following:

- Click **Select Member**. In the Member Selector dialog box, select a Grid member from the list.
- **Graph Configuration**: Select which updates you want to track in the **Updates per Second** graph:
  - **Success**: The number of DDNS update requests that succeeded.
  - **Prerequisite Reject**: The number of DDNS update requests that were rejected because the prerequisite conditions specified in the request were not met.
  - **Reject**: The number of DDNS update requests that were rejected by the DNS service.
  - **Failure**: The number of DDNS update requests that failed.

The widget displays the following information:

- **DDNS Updates tab**: Displays totals for each type of update.
- **Updates per Second tab**: Displays a line graph that tracks the status of the DDNS updates. The time is displayed according to the time zone specified in the User Profile. If the auto-detect time zone option is enabled and Grid Manager cannot determine the browser time zone, then the time is displayed in UTC format. You can mouse over the graph to display the coordinates of any point in the graph.

**System Activity Monitor**

The *System Activity Monitor* widget provides information about the following resources on the selected Grid member: CPU, system memory, NIC usage, and information about VLAN interfaces. By default, the widget displays the system activity of the Grid Master. You can add a *System Activity Monitor* widget to your Dashboard for each Grid member whose resources you want to monitor.

To configure the *System Activity Monitor* widget, click the Configure icon and select a Grid member and the resources that you want to track:

- Click **Select Member**. In the Member Selector dialog box and select a Grid member from the list.
• **CPU**: Select which type of CPU usage you want to track:
  - **User**: The CPU usage of user applications, such as programs and libraries.
  - **System**: The CPU usage of the kernel and drivers.
  - **Idle**: The percentage of CPU that is not in use.

• **System Memory**: Select which portion of the system memory you want to track:
  - **Real Memory Used**: The physical RAM usage.
  - **Swap Used**: The swap area usage. The swap area is the disk area that temporarily holds a process memory image.

• **NIC Usage**: Select how you want to measure network traffic:
  - **Bytes**: Reports the number of bytes.
  - **Packets**: Reports the number of packets.

• **NIC Settings**: Select the port on which you want to measure network traffic. If you have configured VLANs, Grid Manager displays them in the format LAN1 nnnn or LAN2 nnnn, where nnnn represents the associated VLAN ID. For example, a VLAN configured on LAN1 can be displayed as LAN1 297 and a LAN2 VLAN can be LAN2 21. For more information about VLANs, see About Virtual LANs.

The **System Activity Monitor** widget displays a tab for each resource: **CPU, System Memory, and NIC Usage**.

Each tab contains a line graph that tracks the resource utilization per second. The graph in the **CPU** tab tracks the percentage of CPU usage. The graph in the **System Memory** tab tracks the memory utilization percentage. The graph in the **NIC Usage** tab tracks either bytes or packets per second.

The time is displayed according to the time zone specified in the User Profile. If the auto-detect time zone option is enabled and Grid Manager cannot determine the browser time zone, then the time is displayed in UTC format. You can mouse over the graph to display the coordinates of any point in the graph.

**File Distribution Statistics**

The **File Distribution Statistics** widget enables you to monitor the status of file distributions services from the Dashboard. The widget provides an overall status of file distribution on all members in the Grid. It also displays the file system utilization for the file distribution subsystem.

The service status displays one of the following:

- **OK**: All file distribution services are running properly.
- **Stopped**: All file distribution services are stopped.
- **Warning**: The file distribution services are not running properly.
- **Error**: The file distribution services encounter an error.

You can click the link to view detailed information about the file distribution services. Grid Manager displays the Members tab in the File Distribution tab.

To configure the **File Distribution Statistics** widget, click the Configure icon and select one of the following chart types:

- **Pie**
- **Bar**

The **File Distribution Statistics** widget displays the following information:

- **File System Utilization**: The percentage of utilization of the overall allocated file distribution subsystem space on all members. You can use this information to verify if there is sufficient space for file distribution in the Grid.

**Active WebUI Users**

The **Active WebUI Users** widget provides information about the users who are logged in to Grid Manager or System Manager. It does not include users who are using the Infoblox API or are logged in to the serial console.

You can add only one **Active WebUI Users** widget to the Dashboard. You must have a superuser account to add this widget to the Dashboard. It displays the following information about each user:

- **User ID**: The user name.
- **Source Address**: The IP address of the management station the user used to connect to Grid Manager.
- **Logged In Since**: The date and time the user logged in.
- **Idle Time**: The number of minutes the user has not had any activity on Grid Manager. Note that the idle session timeout is 2 hours, so the idle time is cleared every 2 hours.
- **User Agent**: The system used to access Grid Manager, such as the browser version and platform information. You can sort the columns and hide or display each one. You can also export the list to a .csv file.

**Microsoft Servers Status Widget**

The **Microsoft Servers Status** widget displays the operational status of each Microsoft server managed by the Grid. Grid Manager displays this widget only when at least one member in the Grid has a Microsoft management license. You can configure this widget to display the status of all Microsoft servers or only those with warnings and errors. You can also view the monitor and control status for the DNS and DHCP service on the Microsoft server.

To modify the **Microsoft Servers Status** widget, click the Configure icon and select one of the following:

- **Show all Microsoft servers**

Only show servers with service warnings or errors

The Microsoft Servers Status widget displays the following information about each Microsoft server:

- **Server Name**: The hostname of the Microsoft server.
- **IP Address**: The IP address of the Microsoft server.
- **Status**: The connection status of the Microsoft server.
  - **OK**: The Grid member is connected to the Microsoft server.
  - **Connecting**: The Grid member is connecting to the Microsoft server.
  - **Error**: The Grid member tried to connect to the Microsoft server, but failed. You can check the syslog for any messages.
  - **Not Available**: The Microsoft server is disabled. The Grid member does not try to connect to disabled servers.
- **DNS**: The status of the DNS service on the Microsoft server. The DNS service status can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td></td>
<td>The DNS service is functioning properly.</td>
</tr>
<tr>
<td>Red</td>
<td></td>
<td>The Microsoft server is unavailable.</td>
</tr>
<tr>
<td>Yellow</td>
<td></td>
<td>The DNS service is starting or stopping.</td>
</tr>
<tr>
<td>Gray</td>
<td></td>
<td>The DNS service is stopped or management of the Microsoft DNS server is disabled.</td>
</tr>
</tbody>
</table>

- **DHCP**: The status of the DHCP service on the Microsoft server. The DHCP service status can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td></td>
<td>The DHCP service is functioning properly.</td>
</tr>
<tr>
<td>Red</td>
<td></td>
<td>The Microsoft server is unavailable.</td>
</tr>
<tr>
<td>Yellow</td>
<td></td>
<td>The DHCP service is starting or stopping.</td>
</tr>
<tr>
<td>Gray</td>
<td></td>
<td>The DHCP service is stopped or management of the Microsoft DHCP server is disabled.</td>
</tr>
</tbody>
</table>

- **Active Directory Sites**: The status icon in green indicates the synchronization status of Active Directory Sites on the Microsoft server.
- **Enable DNS Monitor & Control**: Displays Yes if the monitor and control status is enabled for the DNS service on the Microsoft server and displays No if it is disabled.
- **Enable DHCP Monitor & Control**: Displays Yes if the monitor and control status is enabled for the DHCP service on the Microsoft server and displays No if it is disabled.

**CSV Import Manager**

CSV Import Manager on the Status Dashboard displays the status of CSV import jobs you have submitted. You can start a file import from CSV Import Manager and control and monitor it from this widget. You can also launch CSV Import Manager from the Task Dashboard or the Toolbar. You can also delete uploaded CSV files. For more information, see About CSV Import. You can click the Refresh icon or configure auto refresh to update the status.

The widget displays the following information about the import jobs that were submitted in the past 30 days:

- **User Name**: The admin user who submitted the CSV import. Only superusers can view this column.
- **Status**: The current status of the import job. The status can be one of the following:
  - **Import successful**: The import is completed without errors. Check the Message field for information about the import.
- **Import unsuccessful**: The import is completed, but with errors. Check the Message field for information about the error message.
- **Import pending**: The job is in queue for execution.
- **Import in progress**: The job is being executed.
- **Import stopped**: The job has been stopped. You can select the job and restart the import.
- **Test successful**: Test is completed without errors. Check the Message field for information about the test.
- **Test unsuccessful**: Test is completed, but with errors. Check the Message field for information about the error message.
- **Test pending**: Test is in queue for execution.
- **Test in progress**: Test is in progress.
- **Test stopped**: Test has been stopped. You can select the job and restart the import.
- **Saved file**: The data file has been uploaded, but the import has not started.

**Note**: After a product restart, which can be caused by a failover, all **Import in progress** jobs go into **Import stopped** state; all **Import pending** jobs continue to be queued for execution.

- **Submitted**: The timestamp when the job was submitted.
- **Completed**: The timestamp when the job was completed. This field is blank if the job has not been completed yet.
- **File Name**: The CSV data file name.
- **Message**: This field displays the number of rows of data that has been processed and the number of rows of data the import has detected errors. Depending on the import options, Grid Manager displays the row number at which it stops the import when it encounters an error, or the total number of rows it has processed by skipping over the erroneous data. For example, if there are 100 rows of data and you select "On error: Stop importing," and there is an error in row 90, the appliance displays 90 of 100 completed, 1 error. If you select "On error: Skip to the next row and continue," the appliance displays 100 of 100 completed, 1 error.
- **FileSize**: The CSV data file size.

**Note**: Superusers can view all CSV import jobs and limited-access users can view only the jobs they submitted.

### Load Balancer Status

The **Load Balancer Status** widget displays the operational status of GLBs (Global Load Balancers) managed by the Grid. Grid Manager displays this widget only when at least one member in the Grid has a Load Balancer license. You can configure this widget to display the status of all GLBs or only those with warnings and errors. To modify the **Load Balancer Status** widget, click the Configure icon and select one of the following:

- **Show all Load Balancers**
- **Only show servers with service warnings or errors**

The **Load Balancer Status** widget displays the following information about each load balancer:

- **Name**: The name of the load balancer.
- **IP Address or FQDN**: The IP address or FQDN of the load balancer.
- **Version**: The TMOS version that is running on the load balancer.
- **Status**: The connection status of the GLB.
  - **OK**: The Grid member is connected to the GLB.
  - **Unknown**: The Grid member is unable to contact the GLB and cannot retrieve any status details. This can be caused by incorrect IP address, FQDN, username, or password.
  - **Error**: The GLB has a connection error. Click the Detailed Status icon to view detailed information or check the syslog for any error messages.
  - **Warning**: Certain issues, such as Grid member failures or licensing issues, have occurred. Click the Detailed Status icon to view detailed information or check the syslog for messages to determine the reason for the warning.
  - **Disabled**: The load balancer is disabled. The Grid member does not try to connect to disabled GLB.

### Pending Approvals

The **Pending Approvals** widget provides information about tasks that are pending your approvals. Add the **Pending Approvals** widget to your Dashboard to monitor tasks that require your approvals.

You can select a task and perform the following:

- **Click the Approve icon to approve the task.**
- **Click the Reject icon to disapprove the task.**

You can also click **Task Manager** to access the **Administration** tab -> **Workflow** tab -> **Task Manager** tab.

The **Pending Approvals** widget displays the following information about each task that requires your approval:

- **Task ID**: The ID associated with the task. The appliance assigns an ID to a task in chronological order.
- **Submitter**: The username of the admin who scheduled or submitted the task.
- **Ticket Number**: The reference number entered by the submitter to identify the task. You can enter up to 20 alphanumeric characters.
- **Scheduled Time**: The date, time, and time zone when the task was scheduled for execution.
- **Affected Object**: The name or value of the object that is associated with the task. For example, if the task involves an A record, this field...
displays the domain name of the record. If it is a fixed address, it displays the IP address of the fixed address.

- **Object Type**: The object type. For example, the appliance can display A Record or Fixed Address.
- **Action**: The operation the appliance performs in this task. The can be: **Add, Modify, Delete, or Network Discovery**.
- **Submit Time**: The date, time, and time zone when the task was submitted. You can select this for display. It is not displayed by default.

**Infoblox Community**

The *Infoblox Community* widget displays the latest news from Infoblox. It provides links to video clips that show you how to perform certain tasks, such as how to prepare for IPAM Express and how to add a network. You can click available links in the widget to get more information about Infoblox products and solutions.

Note that content in the *Infoblox Community* widget may not be displayed in certain versions of Mozilla FireFox, Google Chrome, and Microsoft Internet Explorer due to restrictions these browsers use to block certain secure data.

Follow these steps to unblock the *Infoblox Community* widget and view data in your respective browser:

- **MozillaFireFox**: Click the **Shield icon** in the address bar and choose **DisableProtectiononThisPage** from the drop-down list. The icon in the address bar changes to a warning triangle and content is displayed in the *InfobloxCommunity* widget. For more details, refer to information at [https://blog.mozilla.org/tanvi/2013/04/10/mixed-content-blocking-enabled-in-firefox-23/](https://blog.mozilla.org/tanvi/2013/04/10/mixed-content-blocking-enabled-in-firefox-23/).
- **Google Chrome**: Click the **Shield icon** in the address bar and click **Load unsafe script** in the pop-up box. Chrome automatically refreshes the webpage and loads the content in the *Infoblox Community* widget. For more details, refer to information at [https://support.google.com/chrome/answer/1342714?hl=en](https://support.google.com/chrome/answer/1342714?hl=en).
- **Internet Explorer**: Click the **Compatibility View icon** adjacent to the address bar. The browser refreshes and the *Security Warning* dialog box is displayed. Click **No** in the dialog box. The **Only Secure content is displayed** pop-up blocker is displayed at the bottom of the browser. Click the **Show all content** button in this pop-up blocker to view the content. For more details, refer to the information at [http://windows.microsoft.com/en-in/internet-explorer/use-compatibility-view#ie=ie-8](http://windows.microsoft.com/en-in/internet-explorer/use-compatibility-view#ie=ie-8).

**Mobile Devices Status**

The *Mobile Devices* widget provides information about the number of active leases of the DHCP fingerprint devices managed by the Grid. The widget displays a pie chart indicating the number of active leases in percentile for each of the device category. For information about device category, device class, and device type, see bookmark310. You can click the Refresh icon or configure auto refresh to update the status.

**Note**: The *Mobile Devices* widget updates its data every 15 minutes. A device might not be displayed in this widget if its lease expires within 15 minutes.

To configure the *Mobile Devices* widget, click the Configure icon and do the following:

- Click **Select Network View**. In the **Network View Selector** dialog box, select a network view from the list and click **OK**.

Note that if multiple network views were previously configured, Grid Manager displays the default network view. You can select another network view from the **Network View Selector** dialog box.

The widget displays the number of active leases for the following device classes:

- **MacOS** - Displays all devices that were detected to be running Mac OS.
- **Windows** - Displays all devices that were detected to be running Windows.
- **Android Mobile** - Displays Smartphones/PDAs/Tablets that were detected to be running Android.
- **Apple Mobile** - Displays Smartphones/PDAs/Tablets that were detected to have Apple in the DHCP fingerprint information.
- **No Match** - Displays all devices whose fingerprint information does not match with any of the standard/custom DHCP fingerprint data stored in the appliance. For information about Standard and Custom DHCP Fingerprints, see *Standard and Custom DHCP Fingerprints*.
- **Other** - Displays all devices that belong to a device class other than those listed above.

**Table 2.2 List of device types and classes**

<table>
<thead>
<tr>
<th>Category</th>
<th>Device Class</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Windows</td>
<td>Microsoft Windows 2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Microsoft Windows 2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Microsoft Windows 8</td>
</tr>
<tr>
<td>Mac OS</td>
<td>Macintosh</td>
<td>Apple Mac OS 9</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>----------------</td>
</tr>
<tr>
<td>Apple Mobile</td>
<td>Smartphones/PDAs/Tablets</td>
<td>Apple iPod</td>
</tr>
<tr>
<td>Android Mobile</td>
<td>Smartphones/PDAs/Tablets</td>
<td>Android Phone/Tablet (Generic)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### DNS Integrity Check

The DNSIntegrityCheck widget displays status about DNS data discrepancies that have been detected through DNS integrity check that is designed to mitigate DNS domain hijacking. This widget displays top-level or parent authoritative zones that have been selected for DNS data monitoring. For information about how to configure DNS integrity check to mitigate possible DNS domain hijacking, see [About DNS Integrity Check for Authoritative Zones](#).

The widget displays the following information (note that this table is sorted by **Status**):

- **Critical** (red): Data in the NS RRsets for the authoritative and delegate zones are completely out of synchronization.
- **Severe** (orange): Some data in the NS RRset between the authoritative and delegate zones overlaps and some data is different.
- **Warning** (yellow): The NS RRset for the authoritative zone is a subset of the NS RRset for the delegate zone. It is possible that incorrect IP addresses have been entered at the registrar.
- **Informational** (blue): The NS RRset for the delegate zone is a subset of the NS RRset for the authoritative zone. This could indicate a possible delay in domain registration.
- **Normal** (green): There are no DNS data discrepancies between the NS RRsets for the authoritative and delegated zones.
- **None** (black): No DNS discrepancies data has been collected or DNS integrity check has not been performed.
- **Last Checked**: The timestamp in YYYY-MM-DD HH:MM:SS when the parent domain was last queried for its DNS data.
- **Description**: Information about the zone.

### Previewing Syslog Events

When you select **View Syslog** from the DNS Integrity Check widget for a selected zone, the Syslog Preview dialog is displayed. You can view related syslog events for the selected zone in this dialog, as follows:
- **Timestamp**: The timestamp in YYYY-MM-DD HH:MM:SS when the event was logged.
- **Facility**: The location that determines the processes and daemons from which the log messages are generated.
- **Level**: The severity level of the DNS data discrepancies. This can be **Critical**, **Severe**, **Warning**, **Information**, or **Normal**. For more information, see descriptions for the **Status** field.
- **Server**: The name of the Grid member that performed the data check.
- **Message**: Syslog information about the event. If you have enabled verbose logging, this displays detailed information about the event. For information about how to enable verbose logging, see **Configuring DNS Integrity Check**.

You can also click **Go to Syslog Viewer** on the upper right corner of the dialog to view all events in the syslog. For more information about the syslog, see **Viewing the Syslog**.

### Cloud Statistics

The **Cloud Statistics** widget appears only when you have deployed the Cloud Network Automations license on the Grid Master. This widget displays statistical information for cloud objects. It contains the following tabs: **Tenant & VMs, Fixed vs. Floating** and **Available vs. Allocated**. You must install valid cloud related licenses to access this widget. For more information about installing licenses and enabling Cloud Network Automation, see **Deploying Cloud Network Automation**.

To modify the **Cloud Statistics** widget, click the Configure icon and select one of the following:

- **Show Statistics From**:
  - **All Tenants**: Select this to display statistics for all tenants.
  - **Select Tenant**: Click **Select** to choose a specific tenant for which statistics are displayed.

- **Show**:
  - **All IP Addresses**: Select this to display all IP address allocation for all tenants or the tenant of your choice.
  - **Fixed**: Select this to display only fixed IP address allocation for all tenants or the tenant of your choice. Fixed IP addresses correspond to OpenStack Fixed IP Addresses.
  - **Floating**: Select this to display only floating IP address allocation for all tenants or the tenant of your choice. Floating IP addresses correspond to OpenStack Floating IP Addresses.

### Dig Request

The **Dig Request** widget enables you to perform a DNS lookup on the Grid Master or on the specified Grid member and displays the output of the dig command.

**Note**: When RPZ license is installed on both the Grid Master and the Grid member, the RPZ rule might not be triggered if you perform dig on the Grid member from the Grid Master.

To perform a DNS lookup using the dig command, complete the following:

- **Run dig command on**: Select one of the following. The default is **Grid Master**.
  - **Grid Master**: Select this to perform a DNS lookup on the Grid Master.
  - **Grid Member**: Select this to perform a DNS lookup on the Grid member. Click **Select Member** to select a Grid member. If there are multiple members, the Member Selector dialog box is displayed, from which you can select a member. Click the required member name in the dialog box. You can also click **Clear** to clear the displayed member and select a new one.

- **Name Server to Query (Optional)**: Optionally, specify the name server on which you want to perform a DNS lookup. You can enter either the name, IPv4 address, or IPv6 address of the name server.

- **Record Type**: Select the resource record type from the drop-down list. You can select **Any** to query all the resource record types or select one of the following from the drop-down list: **A, AAAA, CNAME, DNAME, MX, NAPTR, NS, PTR, SRV, TXT, and AXFR**. The default is **Any**.

- **Send Recursive Query**: Select this to send recursive queries for the domain. This check box is selected by default.

- **Domain Name to Query**: Enter the domain name to query.

Click **Perform Dig**. The widget displays the status and output of the dig command. Note that if you have installed RPZ license and enabled RPZ logging in the Grid, you can view RPZ syslog messages by clicking **View RPZ Syslog** if the specified domain name matches the RPZ rule.

### Security Status for Grid

The **Security Status for Grid** widget displays the overall status of Threat Protection, RPZ (Response Policy Zone), and DNS Threat Analytics services on the Grid members that support Infoblox Advanced DNS Protection, hardware or Software ADP, and Infoblox Threat Insight. Grid Manager displays this widget only when at least one member in the Grid has the Threat Protection, RPZ, or Threat Analytics license installed. You can add this widget to the Security dashboard to monitor the overall security status of the Grid. The statistics displayed in this widget are cumulative, collected from all the Grid members that support Infoblox Advanced DNS Protection, hardware or Software ADP, and Infoblox Threat Insight. This widget displays data for the last 30 minutes. The overall status of Threat Protection, RPZ, and DNS Threat Analytics is determined by the threshold values configured in the **Global Dashboard Properties editor**. For information, see **Configuring Security Status Thresholds**.

**Note**: If the Threat Protection license is not installed on any of the Grid members, Grid Manager does not display any threat protection related.
information in this widget. Similarly, if the RPZ license is not installed on any of the Grid members, Grid Manager does not display RPZ and DNS Threat Analytics related information in this widget and if the Threat Analytics license is not installed on any of the Grid members, Grid Manager does not display DNS Threat Analytics related information in this widget.

The widget displays the following information for Threat Protection, RPZ, and DNS Threat Analytics:

- **Status**: Displays the overall status of the security service in the Grid based on the events collected from all the members that support Infoblox Advanced DNS Protection and Infoblox Threat Insight. It represents the status of the most critical member in the Grid.

  - **OK** (Green): The license for the security service is installed and the security service is running. The rulesets for the security service are available and the number of events triggered are less than the yellow and red threshold values configured in the Global Dashboard Properties editor for the corresponding security service.
  - **Warning** (Yellow): The license for the security service is installed and the security service is running. The rulesets for the security service are available and the number of events triggered for any of the parameters equals or exceeds the yellow threshold value, but less than the red threshold value configured in the Global Dashboard Properties editor for the corresponding security service.
  - **Critical** (Red): The license for the security service is installed and the security service is running. The rulesets might not be available or the number of events triggered for any of the parameters, equals or exceeds the red threshold value configured in the Global Dashboard Properties editor for the corresponding security service.
  - **Not Setup** (Black): The license for the security service is installed, but the security service is not running.
  - **Unknown** (Black): The data is not available from the Grid member.


- **Events from <> of <> security capable members**: This column displays the cumulative event counts collected from the online Grid members that support the Infoblox Advanced DNS Protection and Infoblox Threat Insight.
  - **Threat Protection**: Displays the total threat protection event counts for the following severity levels:
    - **Critical** (Red): The total number of critical events.
    - **Major** (Orange): The total number of major events.
    - **Warning** (Yellow): The total number of warning events.
    - **Informational** (Blue): The total number of informational events.
  - **RPZ**: Displays the total number of hits received for the following RPZ rules:
    - **Blocked hits** (Red): Total number of queries that triggered a Block (No Data) or Block (No Such Domain) RPZ rule.
    - **Passthru hits** (Yellow): Total number of queries that triggered a Passthru RPZ rule.
    - **Substituted hits** (Orange): Total number of queries that triggered a Substitute (Domain Name) or Substitute (Record) RPZ rule.
  - **Analytics**: Displays the total number of DNS tunneling events.

- **Definitions/Rules**: This column displays the status of the latest ruleset available in the database. For RPZ, the definition status is based on the latest RPZ feed received from Infoblox specific feeds. You can hover your mouse over the definition status to see the RPZ definition status when RPZ definitions exists.

- **Configuration Status**: This column indicates whether the security service is enabled and running properly or not. Grid manager displays a green check mark if the security service is enabled and running properly in the Grid. If the security service is disabled, a gray pause mark is displayed. You can hover your mouse over the gray pause mark to see the status of the security service.

In addition, you can click the Configure icon and do the following:

- Click **Configure Security Status Thresholds** to configure the thresholds for the security status of the Grid. In the Global Dashboard Properties editor, you can define the threshold values for Threat Protection, RPZ, and DNS Threat Analytics. For information, see Configuring Security Status Thresholds.
- Select the **Auto Refresh Period** check box to turn on auto-refresh and specify the auto-refresh period in seconds. The default auto-refresh period is 30 seconds.

Click the Configure icon again to hide the configuration panel after you complete the modification.

### Security Status for All Members

The **Security Status for All Members** widget displays information about the status of all the Grid members that support Infoblox Advanced DNS Protection, hardware or Software ADP, and Infoblox Threat Insight. Grid Manager displays this widget only when at least one member in the Grid has the Threat Protection or RPZ license. You can add this widget to the Security dashboard to monitor the status of the Grid members that support Infoblox Advanced DNS Protection, hardware or Software ADP, and Infoblox Threat Insight.

**Note**: When an HA Grid Master fails over, the new active node re-collects data from all the Grid members. Hence, it might take a few seconds until the data is displayed in the Security dashboard. When an HA Grid member fails over, the Grid Master stops collecting data from the HA member.

The **Security Status for All Members** widget displays the following information:

- **Overall Status**: The current overall security status of the members that support Infoblox Advanced DNS Protection and Infoblox Threat Insight.

Copyright ©2019, Infoblox, Inc. All rights reserved.
Warning

To Zones
Zone 10
Over Protection
To Dashboard
Critical
Top
by
Refresh
Back
Grid
Members
Status
for
Back
Response
10
Events
Severity
Member Status (System Status)
Security
Go
Member
Critical
Not
To
Grid
Protection
Security
Time:
The status of the threat protection service running on the member. This can be either Rules
Status:
The IPv6 address of the member.
IPv4 Address:
The IPv4 address of the member.
IPv6 Address:
The IPv6 address of the member.
Threat Protection Status:
The status of the threat protection service running on the member. This can be either OK, Warning, Critical, NotSetup, or Unknown. You can hover your mouse over the threat protection status and view the Threat Protection Status for Member widget. For information about the Threat Protection Status for Member widget, see Threat Protection Status for Member.
RPZ Status:
The status of the RPZ service running on the member. This can be either OK, Warning, Critical, NotSetup, or Unknown. You can hover your mouse over the RPZ status and view the ResponsePolicyZone(RPZ) Statistics widget. For information about the Response Policy Zone (RPZ) Statistics widget, see Response Policy Zone (RPZ) Status for Member.
Analytics Status:
The status of the DNS Threat Analytics service running on the member. This can be either OK, Warning, Critical, Not Setup, or Unknown.
You can also do the following in this widget:

- Turn on auto-refresh. Click the Configure icon and select the Auto Refresh Period check box to turn on auto-refresh. Specify the auto-refresh period in seconds. The default auto refresh period is 30 seconds.
- Click the Action icon

(shown as a gear in each row of the table) next to the overall status of each member, and select ViewSyslog to view all the events logged in the syslog. Grid Manager displays the syslog messages in the Syslog Preview window.
- Click the Export icon to export the data displayed in this widget.
- Click the Print icon to print the data displayed in this widget.
- Click Response Policy Zones link in the GoTo field at the top of the widget to view the RPZs configured on the member. Grid Manager displays the Response Policy Zones tab in the DNS tab. To navigate back to the Security dashboard, click Back to Security Dashboard at the top left corner of the navigation bar in the Response Policy Zones tab.
- Click Threat Protection link in the Go To field at the top of the widget to view the threat protection rulesets configured on the member. Grid Manager displays the Threat Protection Rules tab in the Security tab. To navigate back to the Security dashboard, click Back to Security Dashboard at the top left corner of the navigation bar in the Threat Protection Rules tab.
- Click Threat Analytics link in the Go To field at the top of the widget to view the whitelist domains configured on the member. Grid Manager displays the Threat Analytics tab in the Security tab. To navigate back to the Security dashboard, click Back to Security Dashboard at the top right corner of the panel in the Threat Analytics tab.
- Click Members link in the Go To field at the top of the widget to view the members configured in the Grid. Grid Manager displays the Members tab in the Grid Manager tab. To navigate back to the Security dashboard, click Back to Security Dashboard at the top left corner of the navigation bar in the Members tab.

Threat Protection Status for Grid

The Threat Protection Status for Grid widget displays the statistical information about the threat protection events triggered on all the members in the Grid that support Infoblox Advanced DNS Protection, hardware or Software ADP, and Infoblox Threat Insight. This widget contains the following tabs: Total Events by Severity, Top 10 Grid Members, Events Over Time, Top 10 Rules, and Top 10 Clients.

You can do the following in this widget:

- Turn on auto-refresh.
  - Click the Configure icon, select the Auto Refresh Period check box, and specify the refresh period in seconds. The default auto refresh period is 30 seconds.
  - You can click the Configure icon again to hide the configuration panel.
- Click the Total Events by Severity tab to view information about threat protection related events by the severity level. For information, see Total Events by Severity.
- Click the Top 10 Grid Members tab to view information about the top 10 Grid members that have the most number of threat protection events. For information, see Top 10 Grid Members.
- Click the Events Over Time tab to view information about the total event count for each type of event severity in the given time frame. For information, see Events Over Time.
- Click the Top 10 Rules tab to view information about the top 10 threat protection rules with the most number of hits. For information, see Top 10 Rules.
- Click the Top 10 Clients tab to view information about the top 10 clients that have the most number of threat protections events. For information, see Top 10 Clients.

Total Events by Severity

The Total Events by Severity tab displays statistics about the Threat Protection events for each type of event severity. This tab displays a bar chart that lists the total event counts for each severity level. Each severity level is represented by a different color. The event statistics are cumulative, collected from all the members in the Grid that support Infoblox Advanced DNS Protection and Infoblox Threat Insight. This line graph displays the event counts for the following severity levels:
• **Critical** (Red): The total number of critical events.
• **Major** (Orange): The total number of major events.
• **Warning** (Yellow): The total number of warning events.
• **Informational** (Blue): The total number of informational events.

If you have configured a reporting member in the Grid, the **Go To History** link is displayed in this tab. You can click **Go To History** to view the **Threat Protection Event Count By Severity Trend** report in the **Reporting** tab. To navigate back to the Security dashboard from the **Reporting** tab, click **Back to Security Dashboard** at the top left corner of the navigation bar in the **Reporting** tab.

**Top 10 Grid Members**

The **Top 10 Grid Members** tab displays a stacked bar chart that tracks the top Grid members with the most total counts of threat protection events. Each severity level is represented with a different color. The report displays the top 10 members in descending order.

If you have configured a reporting member in the Grid, the **Go To History** link is displayed in this tab. You can click **Go To History** to view the **Threat Protection Event Count By Severity Trend** report in the **Reporting** tab. To navigate back to the Security dashboard from the **Reporting** tab, click **Back to Security Dashboard** at the top left corner of the navigation bar in the **Reporting** tab.

**Events Over Time**

The **Events Over Time** tab displays a line graph that tracks the event count for each event severity in a given time frame. You can view the event counts for the following severity level: Critical, Major, Warning, and Informational. The event statistics are cumulative, collected from all the members in the Grid that supports Infoblox Advanced DNS Protection and Infoblox Threat Insight. Each severity level is represented with a different color.

If you have configured a reporting member in the Grid, the **Go To History** link is displayed in this tab. You can click **Go To History** to view the **Threat Protection Event Count By Severity Trend** report in the **Reporting** tab. To navigate back to the Security dashboard from the **Reporting** tab, click **Back to Security Dashboard** at the top left corner of the navigation bar in the **Reporting** tab.

**Top 10 Rules**

The **Top 10 Rules** tab displays a horizontal bar chart that tracks the top threat protection rules that have the most number of hits. Each severity level is represented with a different color. The report displays the top 10 rules in descending order.

If you have configured a reporting member in the Grid, the **Go To History** link is displayed in this tab. You can click **Go To History** to view the **Threat Protection Top Rules Logged** report in the **Reporting** tab. To navigate back to the Security dashboard from the **Reporting** tab, click **Back to Security Dashboard** at the top left corner of the navigation bar in the **Reporting** tab.

**Top 10 Clients**

The **Top 10 Clients** tab displays a horizontal bar chart that tracks the total number of threat protections events triggered by top clients (source IP addresses). This tab displays the IP addresses of the top 10 clients. For NAT clients, it displays the NAT addresses for the clients.

If you have configured a Reporting member in the Grid, the **Go To History** link is displayed in this tab. You can click **Go To History** to view the **Threat Protection Top Rules Logged by Source** report in the **Reporting** tab. To navigate back to the Security dashboard from the **Reporting** tab, click **Back to Security Dashboard** at the top left corner of the navigation bar in the **Reporting** tab.

**Note:** The data displayed in this widget may not be consistent with the data displayed in the **Threat Protection Top Rules Logged by Source** report.

**Threat Protection Status for Member**

The **Threat Protection Status for Member** widget displays statistics about the threat protection events for a specific Grid member that supports Infoblox Advanced DNS Protection, hardware or Software ADP. For information about the threat protection feature, see [About Infoblox Advanced DNS Protection](#). To configure the **Threat Protection Status for Member** widget, click the Configure icon and complete the following:

- **Click Select Member.** In the **Member Selector** dialog box, select a Grid member from the list that supports Infoblox Advanced DNS Protection, hardware or Software ADP.
- **Select either Dial or Bar as the display format for the following resources:** **Smart NIC CPU, Traffic being dropped, Traffic being received.** Note that Smart NIC CPU selection is displayed only when you select a Grid member that supports Infoblox Advanced DNS Protection.
- **SNIC Settings:** Select the interface for which you want to view the interface usage information. You can select one of the following from the drop-down list: **HA, LAN1, or LAN2.** You can view the interface usage information for the selected interface in the **Interface Usage** tab. This is displayed only when you select a Grid member that supports Infoblox Advanced DNS Protection.
  - Note that you can select the HA port even though the Grid member is not an HA pair, because the HA port on a single member can be exposed to potential attacks.
- **NIC Settings:** Select the interface for which you want to view the interface usage information. You can select one of the following from the...
the drop-down list: HA, LAN1, or LAN2. You can view the interface usage information for the selected interface in the Interface Usage (LAN1) tab. This is displayed only when you select a Grid member that supports Software ADP.

- **Events Over Time**: Select the severity level, Critical, Major, Warning, or Informational, to view the details for a specific severity level. You can select one or all the available severity levels.
- **Select the Auto Refresh Period** check box to turn on auto-refresh, and specify the auto-refresh period in seconds. The default is 30 seconds.

Click the Configure icon again to hide the configuration panel after you complete the modification. You can do the following in this widget:

- **Click the Summary** tab to view the statistics for the following resources in the format you selected:
  - **Smart NIC CPU**: The percentage of Smart NIC CPU that is in use. This is displayed only when you select a Grid member that supports Infoblox Advanced DNS Protection.
  - **Traffic being dropped**: The percentage of traffic dropped. It is displayed for both LAN1 and LAN2 interfaces.
  - **Traffic being received**: The percentage of traffic received. It is displayed for both LAN1 and LAN2 interfaces.

- Click the **Events Over Time** tab to view information about the threat protection event counts for each severity level over the given time frame. It displays line graphs that show the threat protection event counts for each event severity over the last 30 minutes. Each event severity is represented by a different color line graph. You can hover your mouse over the graph to view the coordinates of any point in the graph. You can also click the Events Over Time legend and use it as a filter to view the graph for specific severity level.

- **Click the Top 10 Rules** tab to view information about the threat protection rules that have the most number of hits. It displays a bar chart to track the top 10 threat protection rules with the most number of hits for critical, major, and warning severity levels. Each event severity is displayed in a different color.

If you have configured a Reporting member in the Grid, the **Go To History** link is displayed in this tab. You can click **Go To History** to view the **Threat Protection Top Rules Logged** report in the **Reporting** tab. To navigate back to the Security dashboard from the **Reporting** tab, click **Back to Security Dashboard** at the top left corner of the navigation bar in the **Reporting** tab.

- **Click the Top 10 Clients** tab to view information about the top sources (client IP addresses) that triggered threat protection rules. It displays a bar chart to track the top 10 clients with the most number of hits.

If you have configured a Reporting member in the Grid, the **Go To History** link is displayed in this tab. You can click **Go To History** to view the **Threat Protection Top Rules Logged by Source** report in the **Reporting** tab. To navigate back to the Security dashboard from the **Reporting** tab, click **Back to Security Dashboard** at the top left corner of the navigation bar in the **Reporting** tab.

- **Click the Interface Usage** tab to view information about the interface usage (in megabytes per second) over a given time frame. It displays line graphs that show the interface usage trends for the selected interface over the last 30 minutes. You can hover your mouse over the graph to view the coordinates of any point in the graph.

- **Click the Smart NIC CPU** tab to view the information about the percentage of CPU usage over a given time frame. It displays line graphs that show the CPU usage trends over the last 30 minutes. You can hover your mouse over the graph to view the coordinates of any point in the graph. This is displayed only when you select a Grid member that supports Infoblox Advanced DNS Protection.

Response Policy Zone (RPZ) Status for Grid

The **Response Policy Zone (RPZ) Status for Grid** widget provides statistical information about RPZ hits for the Grid. This widget contains the following tabs: **Top 10 Grid Members**, **RPZ Recent Hits**, **Trend**, and **Health**.

You can do the following in this widget:

- **Select a graph configuration**, **Client Hits**, **Passthru Hits**, **Blocked Hits**, or **Substituted Hits**, to view details of a specific RPZ rule. You can select either one or all the available graph configurations. Note that **Client Hits** is displayed only when the graph type is **Line Diagram**.

- **Select a graph type**, **Stacked Diagram** or **Line Diagram**, to display data in the required diagrammatic format. This option is enabled only when you click the **Trend** tab and disabled when you click the **Top 10 Grid Members**, **RPZ Recent Hits**, or **Health** tabs. For more information, see **Trend**.

- **Click the Top 10 Grid Members** tab to view information about the top 10 Grid members that have the most number of RPZ hits. For more information, see **Top 10 Grid Members**.

- **Click the RPZ Recent Hits** tab to view information about the latest five RPZ hits with unique client addresses. For more information, see **RPZ Recent Hits**.

- **Click the Trend** tab to view RPZ hit statistics for the Grid. For more information, see **Trend**.

- **Click the Health** tab to view information about RPZ zones and their last updated times. For more information, see **Health**.

Note that you must install the RPZ license and enable **RPZ logging** to access this widget. For more information about installing licenses and enabling RPZ logging, see **License Requirements and Admin Permissions** and **Setting DNS Logging Categories**.

Top 10 Grid Members

The **Top 10 Grid Members** tab displays a stacked bar chart that tracks the top Grid members with the most total counts of RPZ hits. Each RPZ hit type is represented with a different color. The report displays the top 10 members in descending order.

RPZ Recent Hits

The **RPZ Recent Hits** tab displays the data that is collected from the most recent hits of five unique clients, identified by their IP addresses, during the last 24 hours. NIOS retrieves this data from the syslog. This tab does not display any data when there are no syslog messages or if RPZ logging is disabled. NIOS displays an error message if RPZ logging is disabled. For more information about enabling RPZ logging, see **Setting DNS Logging Categories**.
Grid Manager retrieves recent hits from the Grid members. If a member has an RPZ license installed, then NIOS will parse the syslog every 60 seconds to collect the data. NIOS parses the generated data to identify the five most recent hits. It searches for these fields in the syslog message: CEF: data string (RPZ syslog) and src fields.

The NIOS appliance remembers the start and end time of previously searched operations to optimize the recent hits data collection, so that the same data is not searched again. Note that when the same client makes repeated queries in the last 24 hours, then there might be less than five unique client hits. You cannot sort or filter values in this tab.

This tab displays the following information:

- **Client IP Address**: IP address of the client that made the recent hits.
- **Requested FQDN**: The domain name or IP address that triggered the RPZ rule. For example, consider an RPZ rule test.com.rpz.com, which queries for test.com. In this example, test.com is the requested FQDN.
- **RPZ Entry**: The RPZ rule that queried a domain name or an IP address. In the above example, test.com.rpz.com is the RPZ rule.
- **Timestamp**: The date and time when the hit occurred.

Consider an example in which you query an RPZ zone and the NIOS appliance logs the following message in the syslog:

```
CEF:0|Infoblox|NIOS|6.9.0-219291|RPZ-QNAME|NODATA|4|app=DNS dst=10.35.101.14 src=10.36.0.251 spt=44460 view=_default qtype=A msg="rpz QNAME NODATA rewrite w18.vg \[A\] via w18.vg.fireeye.com"
```

This tab displays information in the corresponding fields as follows:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client IP Address</td>
<td>Data is retrieved from the src field. Example: 10.36.0.251</td>
</tr>
<tr>
<td>Requested FQDN</td>
<td>It is retrieved from the data between the <code>rewrite</code> and <code>[A] via</code> fields. Example: w18.vg.</td>
</tr>
<tr>
<td>RPZ Entry</td>
<td>It is retrieved from the data after the <code>via</code> field. Example: w18.vg.fireeye.com</td>
</tr>
<tr>
<td>Timestamp</td>
<td>This is listed in the syslog.</td>
</tr>
</tbody>
</table>

You can export data displayed in this tab by clicking the Export icon. For more information, see Exporting Displayed Data.

### Trend

The Trend tab displays statistics of RPZ hits during the last 60 minutes for the Grid. You can use a stacked graph or a line graph to view the hits. Each of the RPZ policy is represented with a different color. This tab displays the following information:

- **Client Hits**: Total number of queries that triggered an RPZ policy. Note that this option is not displayed when you choose Stacked Diagram, but displayed only when you choose Line Diagram.
- **Passthru Hits**: Total number of queries that triggered a Passthru RPZ rule. For more information about passthru rules, see Managing Passthru Rules.
- **Blocked Hits**: Total number of queries that triggered a Block (No Data) or Block (No Such Domain) RPZ rule. For more information, see Managing Block (No Data) Rules or Managing Block (No Such Domain) Rules respectively.
- **Substitute Hits**: Total number of queries that triggered a Substitute (Domain Name) or Substitute (Record) RPZ rule. For more information, see Managing Substitute (Domain Name) Rules and Managing Substitute (Record) Rules.
- **Timestamp**: The graph displays a 24 hours time window. Note the following about this tab:
  - The statistical data in DNS service will be reset when you stop and restart the DNS service or if you force an active DNS service to restart regardless of its state. This results in loss of prior data.
  - Using this graph, you can view the timestamp of statistics collection.

### Health

The Health tab displays information of RPZ zones and their last updated date and time. This data is retrieved directly from the database. Note that you cannot sort or filter values in this tab. You can export the data displayed in this tab by clicking the Export icon. For more information, see Exporting Displayed Data.

### Response Policy Zone (RPZ) Status for Member

The Response Policy Zone (RPZ) Status for Member widget provides statistical information about RPZ hits for the selected member. This widget contains the following tabs: RPZ Recent Hits, Trend, and Health.

You can do the following in this widget:

- **Click Select Member**: In the Member Selector dialog box, choose a Grid member to view the RPZ hits, or statistics, or RPZ zones and their last updated date and time.
- **Select a graph configuration**: ClientHits, Passthru Hits, Blocked Hits, or Substituted Hits, to view details of a specific RPZ rule. You can select either one or all the available graph configurations. Note that Client Hits is displayed only when the graph type is Line Diagram.
m.
- Select a graph type, Stacked Diagram or Line Diagram, to display data in the required diagrammatic format. This option is enabled only when you click the Trend tab and disabled when you click the Top 10 Grid Members, RPZ Recent Hits, or Health tabs. For more information, see Trend.
- Click View Syslog to view the last 20 RPZ events that are logged in the syslog. For more information, see Previewing the Syslog.
- Click the RPZ Recent Hits tab to view information about the latest five RPZ hits with unique client addresses. For more information, see RPZ Recent Hits.
- Click the Trend tab to view RPZ hit statistics on the selected member. For more information, see Trend.
- Click the Health tab to view information about RPZ zones and their last updated times. For more information, see Health.

Note that you must install the RPZ license and enable RPZ logging to access this widget. For more information about installing licenses and enabling RPZ logging, see License Requirements and Admin Permissions and Setting DNS Logging Categories.

### RPZ Recent Hits

The **RPZ Recent Hits** tab displays the data that is collected from the most recent hits of five unique clients, identified by their IP addresses, during the last 24 hours. NIOS retrieves this data from the syslog. This tab does not display any data when there are no syslog messages or if RPZ logging is disabled. NIOS displays an error message if RPZ logging is disabled. For more information about enabling RPZ logging, see Setting DNS Logging Categories.

Grid Manager retrieves recent hits from the selected member. If a member has an RPZ license installed, then NIOS will parse the syslog every 60 seconds to collect the data. NIOS parses the generated data to identify the five most recent hits. It searches for these fields in the syslog message: CEF: data string(RPZ syslog) and src fields.

The NIOS appliance remembers the start and end time of previously searched operations to optimize the recent hits data collection, so that the same data is not searched again. Note that when the same client makes repeated queries in the last 24 hours, then there might be less than five unique client hits. You cannot sort or filter values in this tab.

This tab displays the following information:

- **Client IP Address**: IP address of the client that made the recent hits.
- **Requested FQDN**: The domain name or IP address that triggered the RPZ rule. For example, consider an RPZ rule test.com.rpz.com, which queries for test.com. In this example, test.com is the requested FQDN.
- **RPZ Entry**: The RPZ rule that queried a domain name or an IP address. In the above example, test.com.rpz.com is the RPZ rule.
- **Timestamp**: The date and time when the hit occurred.

Consider an example in which you query an RPZ zone and the NIOS appliance logs the following message in the syslog:

```
CEF:0|Infoblox|NIOS|6.9.0-219291|RPZ-QNAME|NODATA|4|app=DNS dst=10.35.101.14 src=10.36.0.251 spt=44460 view=_default qtype=A msg="rpz QNAME NODATA rewrite w18.vg \[A\] via w18.vg.fireeye.com"
```

This tab displays information in the corresponding fields as follows:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client IP Address</td>
<td>Data is retrieved from the src field.</td>
</tr>
<tr>
<td>Example:</td>
<td>10.36.0.251</td>
</tr>
<tr>
<td>Requested FQDN</td>
<td>It is retrieved from the data between the rewrite and [A] via fields. Example: w18.vg.</td>
</tr>
<tr>
<td>RPZ Entry</td>
<td>It is retrieved from the data after the via field. Example: w18.vg.fireeye.com</td>
</tr>
<tr>
<td>Timestamp</td>
<td>This is listed in the syslog.</td>
</tr>
</tbody>
</table>

### Trend

The **Trend** tab displays statistics of RPZ hits on the selected member during the last 60 minutes. You can use a stacked graph or a line graph to view the hits. DNS service generates RPZ statistics for the selected member. Each of the RPZ policy is represented with a different color. This tab displays the following information:

- **Client Hits**: Total number of queries that triggered an RPZ policy. Note that this option is not displayed when you choose Stacked Diagram, but displayed only when you choose Line Diagram.
- **Passthru Hits**: Total number of queries that triggered a Passthru RPZ rule. For more information about passthru rules, see Managing Passthru Rules.
- **Blocked Hits**: Total number of queries that triggered a Block (No Data) or Block (No Such Domain) RPZ rule. For more information, see Managing Block (No Data) Rules or Managing Block (No Such Domain) Rules respectively.
- **Substituted Hits**: Total number of queries that triggered a Substitute (Domain Name) or Substitute (Record) RPZ rule. For more information, see Managing Substitute (Domain Name) Rules and Managing Substitute (Record) Rules.
- **Timestamp**: The graph displays a 24 hours time window.

Note the following about this tab:

- The statistical data in DNS service will be reset when you stop and restart the DNS service or if you force an active DNS service to restart regardless of its state. This results in loss of prior data.
• Using this graph, you can view the timestamp of statistics collection.

Health

The Health tab displays information of RPZ zones on the selected member and their last updated date and time. This data is retrieved directly from the database. Note that you cannot sort or filter values in this tab. You can export the data displayed in this tab by clicking the Export icon. For more information, see Exporting Displayed Data.

Previewing the Syslog

You can view the RPZ events that are logged in the syslog for a selected Grid member. Note that the preview displays only the last 20 RPZ events from the syslog. This wizard displays the following information:

• Timestamp: The date and time when the hit occurred.
• Facility: The location on the syslog server sorting the log message.
• Level: The severity of the message. This can be ALERT, CRITICAL, DEBUG, EMERGENCY, ERROR, INFO, NOTICE, or WARNING.
• Server: The name of the server that logged this message, plus the process ID.
• Message: Detailed information about the RPZ query. You can click the Go to Syslog Viewer link to view the RPZ events that are logged in the syslog. NIOS displays all the RPZ events that are logged in the syslog for the selected member and the Quick Filter is set to RPZ Incident Logs by default. For more information, see Viewing RPZ in the Syslog.

Tenant & VMs

The Tenant & VMs tab displays a table that shows the total number of Tenants, Cloud VMs, and IP Addresses, depending on your configuration. It also displays the average number of cloud VMs and IP addresses per tenant.

Fixed vs. Floating

The Fixed vs. Floating tab displays IP address allocation for cloud objects. It displays the total number of fixed address allocation and floating address allocation, depending on your configuration. It also displays a pie chart indicating the percentage for each allocation.

Available vs. Allocated

The Available vs. Allocated tab displays IP address allocation for available versus allocated IP addresses. It displays the total number of available IP addresses versus allocated IP addresses, depending on your configuration. It also displays a pie chart indicating the percentage for each allocation.

Threat Analytics Status for Grid

The Threat Analytics Status for Grid widget displays the statistical information about the DNS tunneling events. This widget contains the following tabs: Detections Over Time, Top 10 Grid Members, and Detections.

You can do the following in this widget:

• Turn on auto-refresh.
  • Click the Configure icon, select the Auto Refresh Period check box, and specify the refresh period in seconds. The default auto refresh period is 30 seconds. Click the Configure icon again to hide the configuration panel after you complete the modification.
  • Click the Detections Over Time tab to view information about the detected DNS tunneling events in a given time frame.
  • Click the Top 10 Grid Members tab to view information about the top 10 Grid members with the most total counts of detections by type.
  • Click the Detections tab to view information about all the detected DNS tunneling events.

Detections Over Time

The Detections Over Time tab displays a line graph that tracks the number of detected DNS tunneling events over the given time frame. You can hover your mouse over the graph to view the coordinates of any point in the graph.

Top 10 Grid Members

The Top 10 Grid Members tab displays a stacked bar chart that tracks the top Grid members with the most total counts of detected DNS tunneling events by type. The report displays the top 10 Grid members in descending order.

Detections
The **Detctions** tab displays information about all the detected DNS tunneling events. This tab displays the following information about each detection in table format:

- **Client IP Address**: The IP address of the client.
- **Domain**: The domain name of the client.
- **Timestamp**: The timestamp when the event occurred.
- **Module**: Displays the threat analytics module.

### Threat Analytics Status for Member

The **Threat Analytics Status for Member** widget displays statistics about the DNS tunneling events for a specific Grid member.

To configure the **Threat Analytics Status for Member** widget, click the Configure icon and complete the following:

- **Click Select Member** to select a Grid member. If there are multiple members, the Member Selector dialog box is displayed, from which you can select a member. Click the required member name in the dialog box. You can also click **Clear** to clear the displayed member and select a new one.
- **Select the Auto Refresh Period** check box to turn on auto-refresh, and specify the auto-refresh period in seconds. The default is 30 seconds.

Click the Configure icon again to hide the configuration panel after you complete the modification.

You can do the following in this widget:

- **Click the Detections Over Time tab** to view information about the DNS tunneling event count for the selected Grid member in a given time frame. It displays a line graph that tracks the number of DNS tunneling event detections in a given time frame. You can hover your mouse over the graph to view the coordinates of any point in the graph.
- **Click the Detections tab** to view information about all the detected DNS tunneling events. This tab displays the following information in table format:
  - **Client IP Address**: The IP address of the client.
  - **Domain**: The domain name of the client.
  - **Timestamp**: The timestamp when the event occurred.
  - **Module**: Displays the threat analytics module. This tab displays only the last 15 detections.

### Pool Licenses Statistics

The **Pool Licenses Statistics** widget displays information about pool license allocation in your Grid. Pool licenses are dynamic service and feature licenses, such as vNIOS, DNS, DHCP, and Cloud Platform that you purchase for vNIOS and cloud deployments based on your evolving business needs. The Grid Master keeps track of dynamic licenses that are allocated to vNIOS members and adjusts the total number of available dynamic licenses for each feature and service.

In the widget, you can select the license type and Grid Manager displays the total numbers of assigned and available licenses based on the selected license type.

To configure the **Pool Licenses Statistics** widget, click the Configure icon and complete the following:

- **Show Usage for**: From the drop-down list, select a license type for which you want the appliance to display dynamic license usage.

The widget displays license usage and the numbers of assigned and available licenses.

You can also view the total number of dynamic licenses installed for each feature and service, the number of active and available licenses, their usage, and other related information in the Grid tab -> Licenses tab -> Pool tab of Grid Manager. For information about how to view dynamic licenses, see Managing Dynamic Licenses.

### DNS Record Scavenging

The DNS Record Scavenging dashboard widget displays statistics about the scavenging of stale DNS records. For more information about record scavenging, see DNS Record Scavenging.

The widget displays the following information for the current or last known scavenging activities:

- **Status**: The status of the scavenging operation.
- **Start**: The start time of the scavenging operation.
- **End**: The end time of the scavenging operation.
- **User**: The user who initiated the scavenging operation.
- **Selected Object**: The Grid, view, or zone affected by record scavenging.
- **Action**: The action applied to the scavenging operation.
- **Processed Records**: The number of DNS records processed.
- **Reclaimable Records**: The number of DNS records marked as reclaimable.
- **Reclaimed Records**: The number of DNS records removed during the scavenging operation.

Click an icon on the filter panel, as illustrated in the Figure 2.2, to add a widget to the desired dashboard. Filterpanel is categorized in to the following: Cloud, Security, DNS/DHCP, and Reset. When you click on an icon, Grid Manager displays thumbnails of the widgets belonging to the respective filter. If you click filtersone after the other without clicking Reset, Grid Manager displays thumbnails of all widgets along with the iconthat indicates the category to which the widget belongs. Click Reset to view only those widgets that belong to the selected category.
can also click icon to add a widget to the desired dashboard.

**Reporting Clustering Dashboard**

The **Reporting Clustering Status** dashboard provides detailed information on the status of the entire indexer cluster. You can get information on the status of each peer node, search head, and indexes. You can view the number of peers (reporting members), searchable copies, and number of copies (buckets).

**Note:** The **Reporting Clustering Status** dashboard is available only when you configure the reporting clustering and you must also have the global read-only permissions for Grid Reporting Properties.

The default dashboard includes the following information:

- Indicates whether the reporting data is fully searchable. Displays **Yes** to indicate that all buckets in the cluster have a primary copy.
- Indicates whether the search and replication factors are met.
- Displays the number of indexes and peers that are searchable.

This dashboard might also display the following messages depending on the health of your cluster: Some data is not searchable, All Data is Searchable, Replication factor not met, and Search factor is not met.

**Viewing Reporting Clustering Status**

To view the **Reporting Clustering Status** dashboard:

1. From the **Dashboard** -> **Reporting Clustering Status** tab. In the **Peers** tab, you can view the following information:
   - **Peer Name:** The name of the reporting member.
   - **Fully Searchable:** Indicates whether the peer currently has a complete set of primaries and is fully searchable.
   - **Status:** The status of the reporting member.
   - **Buckets:** The number of copies stored on the peer node. The number of buckets for which the peer has copies

- The **Indexes** tab displays the following information:
  - **Index Name:** The name of the indexer.
  - **Fully Searchable:** Indicates whether the peer currently has a complete set of primaries and is fully searchable.
  - **Searchable Data Copies Status:** The status of the reporting member.
  - **Replicated Data Copies:** The replicated number of copies.
  - **Buckets:** The number of buckets for which the peer has copies.
  - **Cumulative RAW Data Size:** The size of the index, excluding hot buckets.

- The **Search Heads** tab displays the following information:
  - **Search Head Name:** Name of the search head.
  - **Status:** The status of the search head.

**Chapter 3 Smart Folders**

This chapter explains how to create and use smart folders to organize your core network services data. It includes the following sections:

- **About Smart Folders**
  - Global Smart Folders
  - My Smart Folders
  - Predefined Smart Folders
- Creating Smart Folders
- Viewing and Modifying Data in Smart Folders
- Modifying Smart Folders
- Deleting Smart Folders
- Saving a Copy of a Smart Folder
- Printing and Exporting Data in Smart Folders

**About Smart Folders**

Use smart folders to organize your core network services data. Depending on your administrative roles and business needs, you can filter your data by object types, names, extensible attributes, and discovered data such as conflicts, unmanaged data, or the virtual entity data, and then place the filtered results in a smart folder. You can also group the filtered results by defining up to 10 extensible attributes as the Group By rules. For example, you can create a smart folder that contains all the networks you manage in Belgium, and then group the networks by building number, as illustrated in Figure 3.1.

Once you set up a smart folder, the appliance displays up-to-date information based on your filter and grouping criteria each time you access the folder. You can also view and modify object information in the folder. For information, see Viewing and Modifying Data in Smart Folders. With smart folders, you can organize your data in a meaningful way and quickly obtain the information you need to perform specific tasks without searching the entire database.

*Figure 3.1 Creating Smart Folders*
Before you set up your smart folders, decide how you want to organize your data. You can specify search and Group By criteria to help you group information in a meaningful way. You can also decide whether you want to include objects that do not contain attribute values when you use the Group By criteria to group filtered data by extensible attributes. For information, see Creating Smart Folders. Note that a smart folder becomes invalid when you delete an extensible attribute that the folder uses as a filter or Group By criterion. You must redefine the extensible attribute and reconfigure the folder criteria to validate the smart folder.

In Grid Manager, you can create smart folders in both the Global Smart Folders and My Smart Folders panels. In Global Smart Folders, you can create smart folders to which other administrators can create links. Only administrators with superuser accounts can create, edit, and delete global smart folders. For information, see Global Smart Folders. You can create personal folders as well as links to global smart folders in My Smart Folders. For information, see My Smart Folders.

Each smart folder you create can contain up to 2,000 objects. When the number of objects exceeds 2,000, Grid Manager sorts and displays the first 2,000 objects only. It also displays a warning message at the top of the panel. In this case, you may want to redefine your filter criteria to further refine the filtered data in your smart folders.

To create smart folders, follow these procedures:

1. Determine how you want to organize your core network services data.
2. Identify the fields that you want to use to group networks or define extensible attributes for the data that you want to track. For information about extensible attributes, see About Extensible Attributes.

Note: Infoblox strongly recommends that you use Type as one of the filter criteria to improve system performance.

3. Create smart folders in either the My Smart Folders or Global Smart Folders panel. For information, see Creating Smart Folders.

**Global Smart Folders**

You can create global smart folders to share among administrators. You must log in as a superuser account to create, edit, and delete global smart folders. All other users have read-only access to global smart folders. You can create as many folders as you need in Global Smart Folders, but Grid Manager displays a maximum of 500 smart folders in the list panel. You can also save a local copy of an existing folder, depending on your administrative permissions. For information, see Saving a Copy of a Smart Folder.

When you log in as a superuser and mouse over a global smart folder, the following icons appear:

- **Information**: Displays information about the selected smart folder. Information includes comments and filter criteria for the folder. It also displays the Group By rules.
- **Edit**: Click this icon to edit the definition and filter criteria for the smart folder.
- **Create link**: Click this icon to create a link to the smart folder. The link to this folder is placed in My Smart Folders.
- **Delete**: Click this icon to delete the smart folder. This operation does not affect the objects that are in the folder. Only the smart folder is deleted.

**My Smart Folders**

In My Smart Folders, you can create personal smart folders and links to global smart folders. When you create links to global smart folders, you can only view information in the folders. However, you can create a local copy of the global smart folder in its current state for editing purposes. Note that when the original global smart folder is updated, information in your local copy is not updated. For information, see Saving a Copy of a Smart Folder. When you delete a link to a global smart folder in this tab, only the link is deleted. There is no impact on the information in the original global smart folder.

Grid Manager displays a list of smart folders in the list panel. The same list of smart folders is also displayed in the Finder panel. For information,
see Finder Panel.
When you mouse over a smart folder in the list panel, the following icons appear:

- **Information**: Displays information about the selected smart folder. Information includes comments and filter criteria of the folder. It also displays how you grouped the filtered data.
- **Edit**: Click this icon to edit the definition and filter criteria for the smart folder.
- **Delete**: Click this icon to delete the smart folder. This operation does not affect the objects or networks that are in the folder. Only the smart folder is deleted.

### Predefined Smart Folders

The appliance can detect remote clients through their DHCP fingerprints, or through device information discovered through SNMP and other device and network detection protocols. You can use predefined smart folders to view lease history, IP addresses, network infrastructure devices, and other related information for remote clients that contain DHCP fingerprint information related to the following device groups:

- **Smartphone,PDA,Tablet Devices**: Includes all devices that were detected as smartphones, PDAs, and tablets.
- **Microsoft Windows Devices**: Includes all devices that were detected to be running Windows OS.
- **Apple MAC OS Devices**: Includes devices that were detected to be running MAC OS.
- **Conflicts**: Includes hosts detected in the network that have a MAC Address conflict. A discovered host has a MAC address conflict when its MAC address is different from that specified in its fixed address, DHCP lease, or host record.
- **Discovered Routers/Switches**: Includes core network infrastructure devices of the specific Router, Switch, or Switch-Router types discovered by NIOS using the discovery feature set. Clicking on a device name opens the device page under DataManagement→Devices and shows the Interfaces page for the chosen device.
- **Active Directory Sites**: Includes all names that were detected as Active Directory Sites. Clicking on an Active Directory Site opens the Active Directory Site Properties editor where you can edit the name, add, or delete networks that are associated with the Active Directory Site. For more information, see Modifying Active Directory Sites and Networks.
- **Gaming Console Devices**: Includes devices that were detected as gaming consoles.
- **Router and Wireless Access Point Devices**: Includes devices there were detected as routers or wireless access point devices.
- **Unmanaged**: Shows all unmanaged devices.

**Note**: For information about DHCP fingerprints, see About DHCP Fingerprints. For information about discovery, see Infoblox Network Insight

### Creating Smart Folders

You can create personal smart folders in My Smart Folders. You can also create global folders to share among administrators in Global Smart Folders when you log in as a superuser account. Each time you access a smart folder, you obtain up-to-date information about the core network services data that match the filter criteria you set for the folder. You can also set Group By rules to group the filtered data by extensible attributes. Grid Manager displays a hierarchical view of the data using the Group By rules you define.

To create a smart folder:

1. Click the Smart Folders tab.
2. Click the My Smart Folders tab to create a personal smart folder.
   - or
3. If you logged in with a superuser account, click the Global Smart Folders tab to create a global smart folder.
4. Click Create.

4. In the Smart Folder data panel, complete the following:
   - **Name**: Enter the name of the smart folder.
   - **Comment**: Optionally, enter additional information about the smart folder.
   - In the first drop-down list, select a field as the filter. The filter can be a network view or a record type as the filter. Grid Manager highlights extensible attributes and Active Directory Sites in gray. You can also group the default data by adding a Group By rule without adding a filter.

**Note**: Infoblox strongly recommends that you use Type as the first filter criterion to improve system performance.

- In the second drop-down list, select an operator for the filter.
- Enter or select a value for the selected field and operator. Depending on the field and operator that you select, the field can be a text or an integer field. It can also be a drop-down list or a calendar widget. For example, if you select Network/Zone/Range/Member in the Type field, Grid Manager displays all the networks, zones, DHCP ranges, and members in the results table. The results table may display the name in its native characters if the name was originally entered as an IDN (Internationalized Domain Name). For example, the Name column in the results table displays a zone name in Chinese.
- Optionally, click + to add another filter. You can also click Apply to view the filtered data in the results table.
- Optionally, select the Group Results check box to organize the filtered data. You can also disable a Group By filter by deselecting the check box.
- From the Group By drop-down list, select an extensible attribute or an Active Directory Site by which you want to group the filtered data. For example, if you want to group the filtered data by building number, you can select Building from the drop-down list. To add additional Group By rules, click the + icon, and then select a field from the drop-down list. You can apply up to 10 Group By rules. You can also delete a rule by selecting the rule and clicking the - icon.
- After you add all filter criteria and Group By rules, click Apply. Grid Manager displays the filtered data in the results table. Note that in the Name field, the appliance highlights disabled DHCP objects in gray. A DHCP object can be a DHCP range, fixed address,
reservation, host configured for DHCP, or roaming host with an allocated IP address. If you select to include objects with no attribute values in the Group By rules, the appliance may take longer to process the results. You can also choose to display Active Directory Site values in the table.

5. Click Save to save the smart folder.

**Viewing and Modifying Data in Smart Folders**

After you set up a smart folder, the appliance searches for matching objects based on the filter criteria you specified for the folder. Grid Manager also groups the objects by the Group By rules you specify. If you select to include objects with no attribute values, the appliance may take longer to process the results. Each smart folder you create can contain up to 2,000 objects. When the number of objects exceeds 2,000, Grid Manager sorts and displays the first 2,000 objects and a message at the top of the panel. In this case, you may want to redefine your filter criteria to further refine the filtered data in your smart folders.

Grid Manager displays smart folders hierarchically in a tree view based on your Group By rules in the following:

- Smart Folder section in the Finder panel
- Selectors from which you can select a smart folder

In the smart folder list panel however, Grid Manager displays all the smart folders in a flat list. You can modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see *Modifying Data in Tables*.

In the smart folder data panel, Grid Manager displays the first hierarchical level of the smart folder based on your Group By rules. If you do not configure any Group By rule, Grid Manager displays all the objects in the results table. If you select to include objects with no attribute values, Grid Manager also includes these objects in the hierarchical view. Depending on your Group By rules, you can view detailed information about the objects by clicking the object link and drilling down to the lowest hierarchical level, and then opening an object. To go back to a previous hierarchical view, click the link of the corresponding level in the breadcrumb.

To view detailed information about an object:

1. In the Smart Folder data panel, click the object link until you drill down to the last hierarchical level of the folder.
2. Grid Manager displays the following information:
   - **Name**: The name or IP address of the object.
   - **Comment**: Information about the object.
   - **Type**: The object type.
   - **Site**: The site to which the object belongs. This is one of the predefined extensible attributes. You can also select other available extensible attributes for display, and sort the data in ascending or descending order by column.
3. Select an object check box, and then do one of the following:
   - Click the Open icon to display the data in the network list or IP address list.
   - Click the Edit icon to modify or schedule the modification of the object configuration. Grid Manager displays the corresponding editor depending on the object you select.
   - Click the Delete icon to delete the object or click the Schedule Deletion icon to schedule the deletion of the object.

You can also print or export the data in this panel. For information, see *Infoblox Grid Manager*.

**Modifying Smart Folders**

After you create a smart folder, you can modify its filter and grouping criteria. To modify a smart folder:

1. Go to Smart Folders.
2. Click My Smart Folders to modify personal smart folders.
   or
   Click Global Smart Folders to modify global smart folders if you logged in with a superuser account.
3. Mouse over to the smart folder that you want to modify.
4. Click the Edit icon. You can also click the Edit icon next to the name of the smart folder in the data panel.
5. Make the appropriate changes in the Smart Folder data panel as described in *Creating Smart Folders*.

**Deleting Smart Folders**

You can delete personal smart folders in My Smart Folders. However, you must log in as a superuser account to delete global smart folders.

To delete a smart folder:

1. Click the Smart Folders tab.
2. Click the My Smart Folders tab to delete personal smart folders.
   or
   Click the Global Smart Folders tab to delete global smart folders.
3. Mouse over to the smart folder that you want to delete.
4. Click the Delete icon. In the Delete Smart Folder dialog box, click Yes.

**Saving a Copy of a Smart Folder**

You can make a copy of an existing smart folder, add or change filter criteria, and then rename the folder accordingly. You can also create a local copy of the global smart folder in its current state for editing purposes. In My Smart Folders, you can save a folder copy only in My Smart Folders. In Global Smart Folders however, you can save a folder copy in either My Smart Folders or Global Smart Folders. You must have superuser permissions to save a global smart folder copy in Global Smart Folders. Note that when the original global smart folder is updated, information in
To save a copy of a smart folder:

1. Click **My Smart Folders** to save a folder copy in this tab.
   or
   Click **Global Smart Folders** to save a folder copy in either this tab or My Smart Folders. To save a smart folder copy in Global Smart Folders, log in as a superuser account.
2. Select the smart folder that you want to save as a copy.
3. Click **Save copy as**.
4. Grid Manager saves the folder copy in My Smart Folders when you save the folder copy in this tab.
   or
   The **Save Smart Folder As** dialog box appears when you perform this function in Global Smart Folders. Select one of the following:
   - **My Smart Folders**: Saves the copy in My Smart Folders.
   - **Global Smart Folders**: Saves the copy in Global Smart Folders.
   Click **OK**.

**Note:** For the folder copy, the appliance appends the word Copy to the original name of the smart folder. You can change the name of the folder at anytime by editing the folder.

### Printing and Exporting Data in Smart Folders

You can print the list of networks that are on the current smart folder page, or you can export all the data in CSV (comma separated value) format. For information, see **About Tasks** and **Exporting Data to Files**.

## Part 2 Appliance Administration

This section provides information about configuring admin groups, roles, and accounts, and defining the appropriate permissions. It explains how to configure and manage a Grid or an independent appliance, and set operational parameters. It also describes the file distribution services (TFTP, FTP, and HTTP) and the bloxTools environment. It includes the following chapters:

- Chapter 4, **Managing Administrators**,
- Chapter 5, **Deploying a Grid**,
- Chapter 6, **Deploying Independent Appliances**,
- Chapter 8, **Managing Appliance Operations**,
- Chapter 9, **File Distribution Services**,
- Chapter 10, **Managing NIOS Software and Configuration Files**,
- Chapter 11, **bloxTools Environment**,
- Chapter 12, **RIR Registration Updates**,

### Chapter 4 Managing Administrators

This chapter describes the various tasks associated with setting up admin groups, admin roles, admin accounts, and permissions. It contains the following sections:

- **About Admin Accounts**
- **About Admin Groups**
  - Creating Superuser Admin Groups
  - Creating Limited-Access Admin Groups
- **About Admin Roles**
  - Creating Admin Roles
- **Managing Admin Groups and Admin Roles**
  - Modifying Admin Groups and Roles
  - Deleting Admin Groups and Roles
  - Viewing Admin Groups
  - Viewing Admin Roles
  - Viewing Admin Group Assignments
- **About Administrative Permissions**
  - Defining Global Permissions
  - Defining Object Permissions
  - Defining DNS and DHCP Permissions on Grid Members
  - Applying Permissions and Managing Overlaps
  - Managing Permissions
- **Authenticating Administrators**
- **Creating Local Admins**
  - Managing Passwords
  - Modifying and Deleting Admin Accounts
- **About Remote Admins**
- **Authenticating Admins Using RADIUS**
  - Authentication Protocols
• Accounting Activities Using RADIUS
• Configuring Remote RADIUS Servers
• Configuring RADIUS Authentication
• Configuring a RADIUS Authentication Server Group
• Authenticating Admins Using Active Directory
  • Configuring an Active Directory Authentication Service Group
  • Enabling Active Directory Authentication for Nested Groups
• Authenticating Admin Accounts Using TACACS+
  • TACACS+ Accounting
  • Configuring TACACS+
  • Configuring a TACACS+ Authentication Server Group
• Authenticating Admins Using LDAP
  • Authentication Protocols
  • Configuring LDAP
  • Configuring an LDAP Server Group
• Defining the Authentication Policy
  • Configuring a List of Authentication Server Groups
  • Configuring a List of Remote Admin Groups
• Authenticating Admins Using Two-Factor Authentication
  • Best Practices for Configuring Two-Factor Authentication
  • Configuring Certificate Authentication Services
  • Enabling Certificate Authentication Service for a User
  • Viewing Certificate Authentication Services
  • Modifying Certificate Authentication Services
  • Deleting Certificate Authentication Services
• Changing Password Length Requirements
• Notifying Administrators
• Administrative Permissions for Common Tasks
• Administrative Permission for the Grid
  • Administrative Permissions for Grid Members
  • Administrative Permissions for Network Discovery
  • Administrative Permissions for Scheduling Tasks
  • Administrative Permissions for Microsoft Servers
• Administrative Permissions for IPAM Resources
  • Administrative Permissions for IPv4 and IPv6 Networks
• Administrative Permissions for Hosts
• Administrative Permissions for DNS Resources
  • Administrative Permissions for DNS Views
  • Administrative Permissions for Zones
  • Administrative Permissions for Resource Records
  • Administrative Permissions for Adding Blank A or AAAA Records
  • Administrative Permissions for Shared Record Groups
  • Administrative Permissions for DNS64 Synthesis Groups
• Administrative Permissions for DNS Resources with Associated IP addresses in Networks and Ranges on page252
  • Best Practices for Configuring Permissions in Networks and Ranges
  • Changes to Default Behavior
  • Enabling Permissions for DNS Resources in Networks and Ranges
  • Configuring Permissions for DNS Resources in Networks and Ranges
• Administrative Permissions for DHCP Resources
  • Administrative Permissions for Network Views
  • Administrative Permissions for IPv4 and IPv6 Networks and Shared Networks
  • Administrative Permissions for IPv4 or IPv6 Fixed Addresses and IPv4 Reservations
  • Administrative Permissions for IPv4 or IPv6 DHCP Enabled Host Addresses
  • Administrative Permissions for IPv4 and IPv6 DHCP Ranges
  • Administrative Permissions for IPv4 or IPv6 DHCP Templates
  • Administrative Permissions for Roaming Hosts
  • Administrative Permissions for MAC Address Filters
  • Administrative Permissions for the IPv4 and IPv6 DHCP Lease Histories
• Administrative Permissions for File Distribution Services
• Administrative Permissions for Dashboard Tasks
• Administrative Permissions for Certificate Authentication Services and CA Certificates
• Administrative Permissions for Object Change Tracking
• Administrative Permissions for Named ACLs
• Administrative Permissions for DNS Threat Protection
• Administrative Permissions for Threat Analytics service
• Administrative Permissions for Cloud Objects
• Administrative Permissions for Reporting

About Admin Accounts
A user must have an admin account to log in to the NIOS appliance. Each admin account belongs to an admin group, which contains roles and permissions that determine the tasks a user can perform. For information, see About Admin Groups.
When an admin connects to the appliance and logs in with a username and password, the appliance starts a two-step process that includes both authentication and authorization. First, the appliance tries to authenticate the admin using the username and password. Second, it determines the authorized privileges of the admin by identifying the group to which the admin belongs. It grants access to the admin only when it successfully completes this process.

The NIOS appliance can authenticate users that are stored on its local database as well as users stored remotely on an Active Directory domain controller, a RADIUS server, a TACACS+ server or an LDAP server. The group from which the admin receives privileges and properties is stored locally.

NIOS can authenticate users based on X.509 client certificates irrespective of the client certificate source. For example, smart card holders such as U.S. Department of Defense CAC users and PIV card holders. The status of these certificates is stored remotely on OCSP (Online Certificate Status Protocol) responders. NIOS uses two-factor authentication to validate these users. For more information about two-factor authentication and how to configure it, see Authenticating Admins Using Two-Factor Authentication.

The tasks involved in configuring administrator accounts locally and remotely are listed in Table 4.1. Table 4.1 Storing Admin Accounts Locally and Remotely

<table>
<thead>
<tr>
<th>NIOS Appliance</th>
<th>RADIUS server/AD Domain Controller/TACACS+ server/LDAP server/Certificate authentication service</th>
</tr>
</thead>
<tbody>
<tr>
<td>To store admin accounts locally</td>
<td>• Use the default admin group (&quot;admin-group&quot;) or define a new group</td>
</tr>
<tr>
<td></td>
<td>• Set the privileges and properties for the group</td>
</tr>
<tr>
<td></td>
<td>• Add admin accounts to the group</td>
</tr>
<tr>
<td>To store admin accounts remotely</td>
<td>• Configure communication settings with a RADIUS server, an Active Directory domain controller, TACACS+ server, or LDAP server</td>
</tr>
<tr>
<td></td>
<td>If you use admin groups on the RADIUS server, Active Directory domain controller, TACACS+ server, or LDAP server:</td>
</tr>
<tr>
<td></td>
<td>• Configure admin groups that match the remote admin groups</td>
</tr>
<tr>
<td></td>
<td>• Set the privileges and properties for the groups</td>
</tr>
<tr>
<td></td>
<td>If you do not use admin groups on the RADIUS server, Active Directory domain controller, TACACS+ server, or LDAP server:</td>
</tr>
<tr>
<td></td>
<td>• Assign an admin group as the default</td>
</tr>
<tr>
<td></td>
<td>• Configure communication settings with the NIOS appliance</td>
</tr>
<tr>
<td></td>
<td>If you use admin groups:</td>
</tr>
<tr>
<td></td>
<td>• Import Infoblox VSAs (vendor-specific attributes) (if RADIUS)</td>
</tr>
<tr>
<td></td>
<td>• Define an admin group with the same name as that on the NIOS appliance</td>
</tr>
<tr>
<td></td>
<td>• Define admin accounts and link them to an admin group</td>
</tr>
<tr>
<td></td>
<td>If you do not use admin groups:</td>
</tr>
<tr>
<td></td>
<td>• Define admin accounts</td>
</tr>
</tbody>
</table>

The admin policy defines how the appliance authenticates the admin: with the local database, RADIUS, Active Directory, TACACS+, or LDAP. You must add RADIUS, Active Directory, TACACS+, or LDAP as one of the authentication methods in the admin policy to enable that authentication method for admins. See Defining the Authentication Policy for more information about configuring the admin policy.

Figure 4.1 illustrates the relationship of local and remote admin accounts, admin policy, admin groups, and permissions and properties. Figure 4.1 Privileges and Properties Applied to Local and Remote Admin Accounts

Copyright ©2019, Infoblox, Inc. All right reserved.
Complete the following tasks to create an admin account:

1. Use the default admin group or create an admin group. See About Admin Groups.
2. Define the administrative permissions of the admin group. See About Administrative Permissions.
3. Create the admin account and assign it to the admin group.
   - To add the admin account to the local database, see Creating Local Admins.
   - To configure the appliance to authenticate the admin account stored remotely, see About Remote Admins

About Admin Groups

All administrators must belong to an admin group. The permissions and properties that you set for a group apply to all administrators assigned to that group. You can assign a dashboard template to an admin group. A dashboard template specifies the tasks an admin group can access through the Tasks Dashboard tab when they log in to Grid Manager. For information about dashboard templates, see About Dashboard Templates. You can also restrict certain user groups to manage specific tasks in the Tasks Dashboard tab only. These users cannot manage other core network services through Grid Manager. For information about how to apply this restriction, see 4820043.

To define admins who can perform specific core network service tasks, you can set up admin groups and assign them permissions for those tasks. To control when and whether certain tasks should be performed, you can add an admin group to an approval workflow and define the admins as submitters or approvers. A submitter is an admin whose tasks require approvals before execution, and an approver is an admin who can approve the submitted tasks. When you add submitter and approver groups to an approval workflow, you have control over who can perform which mission critical tasks and whether and when the tasks should be executed. For more information about how to create and configure approval workflows, see Configuring Approval Workflows.

There are three types of admin groups:

- **Superuser** – Superuser admin groups provide their members with unlimited access and control of all the operations that a NIOS appliance performs. There is a default superuser admin group, called admin-group, with one superuser administrator, admin. You can add users to this default admin group and create additional admin groups with superuser privileges. Superusers can access the appliance through its console, GUI, and API. In addition, only superusers can create admin groups.

- **Limited-Access** – Limited-access admin groups provide their members with read-only or read/write access to specific resources. These admin groups can access the appliance through the GUI, API, or both. They cannot access the appliance through the console.

- **Default** – When upgrading from previous NIOS releases, the appliance converts the ALL USERS group to the Default Group when the ALL USERS Group contains admin accounts. The appliance does not create the Default Group if there is no permission in the ALL USERS group. The permissions associated with the ALL USERS group are moved to a newly created role called Default Role. Supported in previous NIOS releases, the ALL USERS group was a default group in which you defined global permissions for all limited-access users. This group implicitly included all limited-access users configured on the appliance.

All limited-access admin groups require either read-only or read/write permission to access certain resources, such as Grid members, and DNS and DHCP resources, to perform certain tasks. Therefore, when you create an admin group, you must specify which resources the group is authorized to access and their level of access.

Only superusers can create admin groups and define their administrative permissions. There are two ways to define the permissions of an admin group. You can create an admin group and assign permissions directly to the group, or you can create roles that contain permissions and assign the roles to the admin group.

You must create admin groups and assign them access to the cloud API and applicable permissions so they have authority over delegated
objects. When you assign permissions for objects that have not been delegated, these admin groups or admin users assume applicable permissions to these un-delegated objects. For example, you can create an admin group that can access a specific set of networks while another can access another set of networks. Note that you cannot create a new admin group using the same name. For information about Cloud Network Automation, see Deploying Cloud Network Automation.

Complete the following tasks to assign permissions directly to an admin group:

1. Create an admin group, as described in 4820043
2. Assign permissions to the admin group, as described in About Administrative Permissions. Complete these tasks to assign admin roles to an admin group:
3. Create an admin role, as described in About Admin Roles.
4. Define permissions for the newly created admin role, as described in Creating Admin Roles.
5. Create an admin group and assign the role to the group, as described in 4820043

After you have created admin groups and defined their administrative permissions, you can assign administrators to the group.

- For local admins, see Creating Local Admins.
- For remote admins, see About RemoteAdmins.

Creating Superuser Admin Groups

Superusers have unlimited access to the NIOS appliance. They can perform all operations that the appliance supports. There are some operations, such as creating admin groups and roles, that only superusers can perform. Note that there must always be one superuser admin account, called "admin", stored in the local database to ensure that at least one administrator can log in to the appliance in case the NIOS appliance loses connectivity to the remote admin databases such as RADIUS servers, AD domain controllers, TACACS+ servers, LDAP servers, or OCSP responders.

NIOS comes with a default superuser admin group (admin-group). It also automatically creates a new admin group, fireeye-group, when you add the first FireEye RPZ (Response Policy Zone). Infoblox recommends that you do not add another admin group with the same name as the default or FireEye admin group. Note that the FireEye admin group is read-only and you cannot assign permissions to it. For more information about FireEye RPZs, see About FireEye Integrated RPZs.

When you install valid licenses and configure your Grid for Cloud Network Automation, NIOS enables the cloud-api-only admin group. You can assign admin users to this group so they are authorized to send cloud API requests to the Cloud Platform Appliances. Note that you cannot delete this admin group or create a new admin group using the same name. For information about Cloud Network Automation, see Deploying Cloud Network Automation.

You can create additional superuser admin groups, as follows:

1. From the Administration tab, select the Administrators tab -> Groups tab, and then click the Add icon.
2. In the Add Admin Group wizard, complete the following:
   - Name: Enter a name for the admin group.
   - Comment: Enter useful information about the group, such as location or department. For fireeye-group, NIOS displays Group used to receive FireEye alerts in this field.
   - Disable: Select this to retain an inactivated profile for this admin group in the configuration. For example, you may want to define a profile for recently hired administrators who have not yet started work. Then when they do start, you simply need to clear this check box to activate the profile.
3. Click Next and complete the following:
   - Superusers: Select this to grant the admin accounts that you assign to this group full authority to view and configure all types of data and perform all tasks.
   - Allowed Interfaces: Superusers admin groups are automatically granted access to the Infoblox GUI (Grid Manager) and API. You can specify which API the superusers group can access. Note that you must have the Cloud Network Automation or Cloud Platform license installed to configure access to the cloud API.
   - GUI: This is selected by default. The superusers admin automatically has full access to Grid Manager.
   - API: This is selected by default. Note that the following options are displayed only if a cloud license is installed in the Grid.
     - API (WAPI/PAPI only): The superusers admin group has full access to the RESTful API and the Infoblox API by default.
     - Cloud API: Select this to allow the superusers admin group to use the cloud API. This option is available only if a cloud license is installed in the Grid. Select one of the following:
       - Cloud API only (no PAPI): Select this to allow the admin group to use WAPI (RESTful API) to send cloud API requests. Note that the Cloud API uses WAPI exclusively. The group has no access to the Infoblox API.
       - Cloud API and PAPI (No WAPI): Select this to allow the admin group to send API requests and have access to the Infoblox API. However, the group cannot use WAPI to send cloud API calls.

Note: When you assign cloud API access to an admin group, the group assumes full authority over all delegated objects. You must however specifically assign object permissions to the admin group for the group to gain authority over non-delegated objects. For information about how to assign object permissions, see Defining Object Permissions.

4. Click Next and complete the following to define the dashboard template:
   - Dashboard Template: From the drop-down list, select the dashboard template you want to assign to this superuser group. When you apply a dashboard template to an admin group, the template applies to all users in the group. The default is None, which means that users in this group can access all licensed tasks in the Tasks Dashboard tab if they have the correct permissions to the task-related objects. Note that if you want to delete a template, you must first unassign the template from an admin group, or select None, before you can delete it. For more information about dashboard templates, see About Dashboards.
5. Click **Next** to add admin email addresses if you want the appliance to send approval workflow notifications to a list of email addresses for the admin group. Complete the following in the Email Address table:

Click the Add icon and Grid Manager adds a row to the table. Enter the email address of the admin who should receive workflow notifications. You can click the Add icon again to add more email addresses. You can also select an email address and click the Delete icon to delete it. To modify an email address, click the **Email Address** column and modify the existing address.

**Note:** When you configure an approval workflow and select **Group Email Address(es)** as the approver notification addresses, the appliance sends workflow notifications to all email addresses you have added to this table. For information, see Configuring Approval Workflows.

6. Optionally, click **Next** to add extensible attributes to the admin group. For information, see About Extensible Attributes.

7. Save the configuration and click **Restart** if it appears at the top of the screen. You can do one of the following after you create a superuser admin group:

- Add local admins to the superuser group. For information, see Creating Local Admins.
- Assign the superuser group to remote admins. For information, see About Remote Admins.

Creating Limited-Access Admin Groups

When you create a limited-access admin group, you can assign roles to it. The group then inherits the permissions of its assigned roles. In addition, you can assign permissions directly to the group. Only superusers can create admin groups.

To create a limited-access admin group:

1. From the **Administration** tab, select the **Administrators** tab -> **Groups** tab, and then click the Add icon.
2. In the **Add Admin Group** wizard, complete the following:
   - **Name:** Enter a name for the admin group.
   - **Comment:** Enter useful information about the group, such as location or department.
   - **Disable:** Select this to retain an inactivated profile for this admin group in the configuration. For example, you may want to define a profile for recently hired administrators who have not yet started work. Then when they do start, you simply need to clear this check box to activate the profile.
3. Click **Next** and complete the following:
   - **Superusers:** Clear this check box to create a limited-access admin group.
   - **Roles:** Optionally, click the Add icon to add an admin role to the admin group. In the **Role Selector** dialog box, select the roles you want to assign to the admin group, and then click the Select icon. Use Shift+click and Ctrl+click to select multiple admin roles. You can assign up to 21 roles to a admin group. The appliance displays the selected roles in the list box. When an admin group is assigned multiple roles, the appliance applies the permissions to the group in the order the roles are listed. Therefore if there are overlapped permissions among the roles, the appliance uses the permission from the role that is listed first and ignores the others. You can reorder the list by selecting a role and clicking the arrow keys to move the role up and down the list. To delete a role, select it and click the Delete icon.
   - **Allowed Interfaces:** Specify whether the admin group can use the Infoblox GUI (Grid Manager) and the API (application programming interface) to configure the appliance. Note that you must have the Cloud Network Automation or Cloud Platform license installed to configure access to the cloud API.
     - **GUI:** Select this to allow the admin group to use the Infoblox GUI, Grid Manager.
     - **API:** Select this to allow the admin group access to the Infoblox API. The following options are available only if a Cloud Network Automation or Cloud Platform license is active in the Grid. You must first select this option to enable the following options.
       - **API (WAPI/PAPI only):** Select this to allow the admin group to use only the RESTful API and Infoblox API.
       - **Cloud API:** Select this to allow the admin group to use the cloud API. This option is available only if a Cloud Network Automation or Cloud Platform license is installed in the Grid. Select one of the following:
         - **Cloud API only (No PAPI):** Select this to allow the admin group to use WAPI (RESTful API) to send cloud API requests. Note that the Cloud API uses WAPI exclusively. The group has no access to the Infoblox API.
         - **Cloud API and PAPI (No WAPI):** Select this to allow the admin group to send API requests and have access to the Infoblox API. However, the group cannot use RESTful API to send cloud API calls.

**Note:** When you assign cloud API access to an admin group, the group assumes full authority over all delegated objects. You must however specifically assign object permissions to the admin group for the group to gain authority over non-delegated objects. For information about how to assign object permissions, see Defining Object Permissions.

4. Click **Next** and complete the following to define the dashboard template:

   - **DashboardTemplate:** From the drop-down list, select the dashboard template you want to assign to this superuser group. When you assign a dashboard template to an admin group, the template applies to all users in the group. The default is None, which means that users in this group can perform all licensed tasks in the **TasksDashboard** tab if they have the correct permissions to the task-related objects. Note that if you want to delete a template, you must first unassign the template from an admin group, or select None, before you can delete it. For more information about dashboard templates, see About Dashboards.
   - **Display Task flow Dashboards Only:** Select this check box if you want to restrict this admin group to access only the Tasks Dashboard in Grid Manager. Note that when you select this check box, users in this admin group have access to the tasks you specified in the selected dashboard template, if applicable. They cannot perform any other tasks or manage any core network services in Grid Manager the next time they log in to the system.

---

Copyright ©2019, Infoblox, Inc. All rights reserved.
5. Click **Next** to add admin email addresses if you want the appliance to send approval workflow notifications to a list of email addresses for the admin group. Complete the following in the Email Address table:

Click the **Add** icon and Grid Manager adds a row to the table. Enter the email address of the admin who should receive workflow notifications. You can click the **Add** icon again to add more email addresses. You can also select an email address and click the **Delete** icon to delete it. To modify an email address, click the **Address** column and modify the existing address.

**Note:** When you configure an approval workflow and select **Group Email Address(es)** as the approver notification addresses, the appliance sends workflow notifications to all email addresses you have added to this table. For information, see *Creating Approval Workflows.*

6. Optionally, click **Next** to add or delete extensible attributes for this admin group. For information, see *About Extensible Attributes.*

7. Save the configuration and click **Restart** if it appears at the top of the screen.

### About Admin Roles

An admin role is a group of permissions that you can apply to one or more admin groups. Roles allow you to quickly and easily apply a suite of permissions to an admin group. You can define roles once and apply them to multiple admin groups. The appliance contains the following system-defined admin roles:

- **DHCP Admin:** Provides read/write access to all network views, all DHCP MAC filters, all Grid members, and all Microsoft servers that are managed by the Grid. It also provides read-only access to all DHCP templates and DHCP lease history.
- **DNS Admin:** Provides read/write access to all Grid members, all Microsoft servers that are managed by the Grid, all shared record groups, and all DNS views.
- **DTC Admin:** Provides read/write access to all DTC objects, such as LBDNs, LBDN records, pools, servers, monitors, certificates, GeoIP, and topologies.
- **File Distribution Admin:** Provides read/write access to Grid file distribution properties.
- **Grid Admin:** Provides read/write access to all DNS views, all shared record groups, all members, all Microsoft servers that are managed by the Grid, all network views, all DHCP MAC filters, all DHCP templates, DHCP lease history, Grid File distribution properties, network discovery, task scheduling, and all Dashboard tasks.
- **Load Balancer Admin:** Provides read/write access to all load balancer resources.
- **PKI Admin:** Provides read/write access to all HSM groups, all certificate authentication services, and all CA certificates.
- **DHCP Fingerprint:** Provides read/write access to all DHCP fingerprint related objects.

You can assign these system-defined roles to admin groups and create additional roles based on the job functions in your organization. If you are creating a role that has similar permissions to an existing role, you can copy the role and then make the necessary modifications to the new role. Thus, you do not have to create each new role from scratch.

You can assign up to 21 roles to an admin group, and you can assign a role to more than one admin group. When you make a change to a role, the appliance automatically applies the change to that role in all admin groups to which the role is assigned.

### Creating Admin Roles

There are two ways to create an admin role. You can create a new role and define its permissions, or you can copy an existing role and redefine the configuration for the new role.

To create a new role from scratch:

1. From the **Administration** tab, select the **Administrators** tab -> **Roles** tab, and then click the **Add** icon.
2. In the **Add Role** wizard, complete the following:
   - **Name:** Enter a name for the role.
   - **Comment:** Enter useful information about the role. For example, if you are creating a role for IT personnel, you can put the information here.
   - **Disable:** Select this to retain an inactivated profile for this admin role in the configuration.
3. Optionally, click **Next** to add extensible attributes to this role. For information, see *About Extensible Attributes.*
4. Click **Next** and select one of the following:
   - **Save & Add Permissions:** Save the entry and add permissions to the role. Grid Manager displays the **Permissions** tab with the newly created role selected. You can then add permissions to this role. For information, see *About Administrative Permissions.*
   - **Save & Close:** Save the entry and close the wizard.
   - **Save & Edit:** Save the entry and continue to edit.
   - **Save & New:** Save the entry and open a new wizard.

To copy an existing role:

1. From the **Administration** tab, select the **Administrators** tab -> **Roles** tab -> **admin_role** check box, and then click **Clone** from the **Toolbar**.
2. The **Copy Role** editor provides the following tabs from which you can modify data for the new role:
   - **General:** Enter the name and information about the new role. You can also disable the role in this tab.
   - **Admin Groups:** Displays a list of admin groups that are currently using this role. You cannot modify the list.
   - **Extensible Attributes:** Add and delete extensible attributes that are associated with the admin role. You can also modify the values of the extensible attributes. For information, see *About Extensible Attributes.*
3. Save the configuration and click **Restart** if it appears at the top of the screen. The appliance displays the new role in the **Roles** tab.
• Define their permissions. For information and guidelines on defining permissions, see About Administrative Permissions.
• Assign roles to admin groups, as described in Creating Limited-Access Admin Groups.

Managing Admin Groups and Admin Roles

After you create an admin group or an admin role, you can view, modify, and delete it.

Modifying Admin Groups and Roles

To modify an admin group:

1. From the Administration tab, select the Administrators tab -> Groups tab -> admin_group check box, and then click the Edit icon.
2. The Admin Group editor provides the following tabs from which you can modify data:

   • General: You can modify the following data.
     • Name: Modify the name of the admin group.
     • Comment: Enter useful information about the group, such as location or department.
     • Disable: Select this to retain an inactivated profile for this admin group in the configuration. For example, you may want to define a profile for recently hired administrators who have not yet started work. Then when they do start, you simply need to clear this check box to activate the profile.
     • Allow Access from: To control access to the GUI and API, select one of the following. You can restrict access using a named ACL or define individual ACEs. For information about named ACLs, see Configuring Access Control.

Note: This group-based authentication is applicable for Grid-wide settings only. NIOS authenticates user credentials only after it authenticates the Network: Modify the data as described in Limited-Access IPv6 Admin.

3. Save the configuration and click Restart if it appears at the top of the screen.

Deleting Admin Groups and Roles

You can remove any default or custom admin group as long as it is not your own admin group or the last admin group. You can also delete any default or custom admin role. The appliance puts the deleted roles in the Recycle Bin, if enabled.

Note: You cannot delete the cloud-api-only and splunk-reporting-group admin groups. These admin groups are automatically created when you configure your Grid for Cloud Network Automation and Reporting and Analytics respectively. For information about Cloud Network Automation and Reporting and Analytics, see Deploying Cloud Network Automation and Infoblox Reporting and Analytics.

To delete an admin group:

1. From the Administration tab, select the Administrators tab -> Groups tab -> admin_group check box, and then click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes.
3. From the Administration tab, select the Administrators tab -> Roles tab -> admin_role check box, and then click the Delete icon.

Copyright ©2019, Infoblox, Inc. All right reserved.
Viewing Admin Groups

You can view the list of admin groups that are currently in the Grid. To view admin groups, from the Administration tab, select the Administrator tab -> Groups tab.

Grid Manager displays the following information:

- **Name**: The name of the admin group.
- **Superuser**: Indicates whether the admin accounts that you assign to this group have full authority to view and configure all types of data. The value can be Yes or No.
- **Comment**: The information about the admin group. You can select the additional fields, Disabled and Site, for display.
- You can also do the following:
  - Sort the data in ascending or descending order by column.
  - Use filters and the Goto function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Goto field and select the object from the possible matches.
  - Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
  - Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
  - Print or export the data.

Viewing Admin Roles

You can view the list of admin roles that are currently in the Grid. To view admin roles, from the Administration tab, select the Administrators tab -> Roles tab.

Grid Manager displays the following information:

- **Name**: The name of the admin role.
- **System**: Indicates whether the admin role is system defined or not. The value can be Yes or No.
- **Comment**: The information about the admin role.

You can select the additional fields, Disabled and Site, for display. You can also do the following:

- Sort the data in ascending or descending order by column.
- Use filters and the Goto function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Goto field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
- Print or export the data.

Viewing Admin Group Assignments

After you define permissions for an admin role, you can assign it to multiple admin groups. You can view the list of admin groups to which an admin role is assigned, as follows:

1. From the Administration tab, select the Administrators tab -> Roles tab -> admin_group check box, and then click the Edit icon.
2. In the Role editor, select the Admin Groups tab.

Grid Manager displays the list of admin groups to which the role is assigned.

About Administrative Permissions

You can assign permissions to admin roles which you then assign to admin groups, or you can assign permissions directly to an admin group.

The following are permissions you can grant admin groups and roles:

- **Read/Write (RW)**: Allows admins to add, modify, delete, view, and search for a resource.
- **Read-Only (RO)**: Allows admins to view and search for a resource. Admins cannot add, modify, or delete the resource.
- **Deny**: Prevents admins from adding, modifying, deleting, and viewing a resource. This is the default permission level for all resources.

By default, the superuser group (admin-group) has full access to all resources on the appliance. Superusers can create limited-access admin groups and grant them permissions to resources at the global and object levels.

Limited-access admin groups must have either read-only or read/write permissions assigned in order to view information or perform tasks on any supported objects.

When you assign permissions at the global level, the permissions apply to all objects that belong to the specified resource. For example, when you define a read/write permission to all DHCP networks, the permission applies to all DHCP ranges and fixed addresses in the networks. For information about global permissions, see bookmark411 bookmark411.

You can also define permissions at a more granular level, such as for a specific Grid member, DNS zone, Response Policy Zone, network, and...
even an individual database object, such as a resource record or fixed address. When you define a permission at the object level, admins with this permission can only manage the specified object and its associated objects. For information about object permissions, see bookmark415. You can use global and object permissions to restrict admins to specific DNS and DHCP resources on specific Grid members by assigning the appropriate permissions. You can use this feature to separate DNS and DHCP administration on selected Grid members. For more information, see bookmark419.

You can configure global permissions, object permissions, and member DNS and DHCP permissions for default and custom admin groups and roles. You cannot however define permissions for the factory default roles, such as DHCP Admin.

The appliance supports the following permissions:

- Grid permissions: Includes Grid DNS properties, Grid DHCP properties, all Grid members, Microsoft servers that are managed by the Grid, network discovery, task scheduling, CSV imports, and all dashboard tasks.
- IPAM permissions: Includes network views, IPv4 and IPv6 networks, and host records.
- DHCP permissions: Includes Grid DHCP properties, network views, IPv4 networks, host records, DHCP ranges, DHCP fixed addresses/reservations, DHCP enabled host addresses, Mac filters, shared networks, DHCP templates, lease history, and roaming hosts.
- DNS permissions: Includes Grid DNS properties, DNS views, DNS zones, Response Policy Zones, host records, bulk hosts, all DNS resource records, all shared records, and adding a blank A/AAAA record.
- File distribution permissions: Includes Grid-level file distribution properties.
- Reporting permissions: Includes Grid-level reporting properties.
- Administration permissions: Includes all certificate authentication services, CA certificates and object change tracking.
- GLB (Global Load Balancer) permissions: Includes all NIOS managed GLB objects.
- DHCP fingerprint permissions: Includes all DHCP fingerprint related objects.
- Named ACL permissions: Includes all named ACLs (access control lists).
- Cloud permissions: Includes all tenant objects.

NIOS applies permissions hierarchically in a parent-child structure. When you define permissions for a resource, all objects within that resource inherit the same permissions. For example, when you grant an admin group read/write permission for a network, the admin group automatically has read/write permission for objects in that network. To override permissions set at a higher level, you define permissions at a more specific level. For example, you can override the read/write network-level permission by setting read-only or deny permission for a fixed address or a DHCP-enabled host address. To define permissions for a more specific level, see the following:

- Permissions for common tasks, as described in Administrative Permissions for Common Tasks.
- Permissions for the Grid and Grid members, as described in Administrative Permission for the Grid.
- Permissions for IPAM resources, such as IPv6 networks, as described in Administrative Permissions for IPAM Resources.
- Permissions for DNS resources, such as DNS views and A records, as described in Administrative Permissions for DNS Resources.
- Permissions for DNS resource with associated IP addresses in networks and ranges, as described in Administrative Permissions for DNS Resources with Associated IP addresses in Networks and Ranges.
- Permissions for DHCP resources, such as network views and fixed addresses, as described in Administrative Permissions for DHCP Resources.
- Permissions for file distribution services, as described in Administrative Permissions for File Distribution Services.
- Permissions for certificate authentication services and CA certificates, as described in Administrative Permissions for Certificate Authentication Services and CA Certificates.
- Permissions for object change tracking, as described in Administrative Permissions for Object Change Tracking.
- Permissions for GLB and GLB objects, as described in Administrative Permissions for Load Balancers.
- Permissions for Cloud objects, as described in Administrative Permissions for Cloud Objects.

When you set permissions that overlap with existing permissions, Grid Manager displays a warning about the overlaps. You can view detailed information and find out which permissions the appliance uses and which ones it ignores. For information, see bookmark423.

**Defining Global Permissions**

You can define permissions at a global level for an admin group or admin role. To define global permissions:

1. For an admin group: From the Administration tab, select the Administrators tab -> Permissions tab -> admin_group in the Groups table, and then click the Add icon -> Global Permissions from the Create New Permission area or select Add -> Global Permissions from the Toolbar.
   
2. For an admin role: From the Administration tab, select the Administrators tab -> Permissions tab -> admin_role in the Roles table, and then click Add icon -> Global Permissions from the Create New Permission area or select Add -> Global Permissions from the Toolbar.

2. Grid Manager displays the Manage Global Permissions editor. For an admin group, the appliance displays the selected admin group in the Group Permission field. For an admin role, the appliance displays the selected admin role in the Role Permission field. You can also select a different group or role from the drop-down list.

3. Select the resources that you want to manage from the Permission Type drop-down list. Depending on your selection, Grid Manager displays the corresponding resources for the selected permission type in the table.

4. Select Read/Write, Read-Only, or Deny for the resources you want to configure. By default, the appliance denies access to resources if you do not specifically configure them.

5. Optionally, select additional resources from the Permission Type drop-down list. Grid Manager appends the new resources to the ones that you have already configured. Define the permissions for the resources you select.

6. Save the configuration and click Restart if it appears at the top of the screen.

*Table 4.2* lists global permissions you can assign to admin groups or admin roles:

**Copyright ©2019, Infoblox, Inc. All right reserved.**
## Table 4.2 Global Permissions

<table>
<thead>
<tr>
<th>Permissions (Read/Write, Read-Only, or Deny)</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Permissions</td>
<td>All Certificate Authentication Services</td>
<td>For more information, see <a href="#">Administrative Permissions for Certificate Authentication Services and CA Certificates</a>.</td>
</tr>
<tr>
<td></td>
<td>All CA Certificates</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Object Change Tracking</td>
<td>For more information, see <a href="#">Administrative Permissions for Object Change Tracking</a>.</td>
</tr>
<tr>
<td>Cloud Permissions</td>
<td>All Tenants</td>
<td>For more information, see <a href="#">Administrative Permissions for Cloud Objects</a>.</td>
</tr>
<tr>
<td>Named ACL Permissions</td>
<td>Named ACL</td>
<td>For more information, see <a href="#">Administrative Permissions for Named ACLs</a>.</td>
</tr>
<tr>
<td>DHCP Permissions</td>
<td>Grid DHCP Properties</td>
<td>For more information, see <a href="#">Administrative Permissions for Common Tasks</a>.</td>
</tr>
<tr>
<td></td>
<td>All Network Views</td>
<td>For more information, see <a href="#">Administrative Permissions for Network Views</a>.</td>
</tr>
<tr>
<td></td>
<td>All IPv4/IPv6 Networks</td>
<td>For more information, see <a href="#">Administrative Permissions for IPv4 and IPv6 Networks and Shared Networks</a>.</td>
</tr>
<tr>
<td></td>
<td>All Hosts</td>
<td>For more information, see <a href="#">Administrative Permissions for Hosts</a>.</td>
</tr>
<tr>
<td></td>
<td>All DHCP Fingerprints</td>
<td>For more information, see <a href="#">Administrative Permissions</a>.</td>
</tr>
<tr>
<td></td>
<td>All DHCP MAC Filters</td>
<td>For more information, see <a href="#">Administrative Permissions for MAC Address Filters</a>.</td>
</tr>
<tr>
<td></td>
<td>All IPv4/IPv6 DHCP Fixed Addresses/Reservations</td>
<td>For more information, see <a href="#">Administrative Permissions for IPv4 or IPv6 Fixed Addresses and IPv4 Reservations</a>.</td>
</tr>
<tr>
<td></td>
<td>All IPv4/IPv6 Host Addresses</td>
<td>For more information, see <a href="#">Administrative Permissions for IPv4 or IPv6 DHCP Enabled Host Addresses</a>.</td>
</tr>
<tr>
<td></td>
<td>All IPv4/IPv6 Ranges</td>
<td>For more information, see <a href="#">Administrative Permissions for IPv4 and IPv6 DHCP Ranges</a>.</td>
</tr>
<tr>
<td></td>
<td>All IPv4/IPv6 Shared Networks</td>
<td>For more information, see <a href="#">Administrative Permissions for IPv4 and IPv6 Networks and Shared Networks</a>.</td>
</tr>
<tr>
<td></td>
<td>All IPv4/IPv6 DHCP Templates</td>
<td>For more information, see <a href="#">Administrative Permissions for IPv4 or IPv6 DHCP Templates</a>.</td>
</tr>
<tr>
<td></td>
<td>All Microsoft Superscopes</td>
<td>For more information, see <a href="#">Administrative Permissions for IPv4 or IPv6 DHCP Templates</a>.</td>
</tr>
<tr>
<td></td>
<td>All Roaming Hosts</td>
<td>For more information, see <a href="#">Administrative Permissions for Roaming Hosts</a>.</td>
</tr>
<tr>
<td>DNS Permissions Grid</td>
<td>DNS Properties</td>
<td>For more information, see <a href="#">Administrative Permissions for Common Tasks</a>.</td>
</tr>
<tr>
<td></td>
<td>All DNS Views</td>
<td>For more information, see <a href="#">Administrative Permissions for Common Tasks</a>.</td>
</tr>
<tr>
<td></td>
<td>All DNS Zones</td>
<td>For more information, see <a href="#">Administrative Permissions for Common Tasks</a>.</td>
</tr>
<tr>
<td></td>
<td>All Hosts</td>
<td>For more information, see <a href="#">Administrative Permissions for Hosts</a>.</td>
</tr>
<tr>
<td></td>
<td>All IPv4/IPv6 Host Addresses</td>
<td>For more information, see <a href="#">Administrative Permissions for DNS Resources with Associated IP addresses in Networks and Ranges</a>.</td>
</tr>
<tr>
<td></td>
<td>All Resource Records (A, AAAA, CNAME, DNAME, NAPTR, MX, PTR, SRV, TXT, TLSA and Bulkhost)</td>
<td>For more information, see <a href="#">Administrative Permissions for Common Tasks</a>.</td>
</tr>
<tr>
<td></td>
<td>All Shared Record Groups</td>
<td>For more information, see <a href="#">Administrative Permissions for Shared Record Groups</a>.</td>
</tr>
<tr>
<td></td>
<td>All Shared Records (A, AAAA, MX, SRV and TXT)</td>
<td>For more information, see <a href="#">Administrative Permissions for Common Tasks</a>.</td>
</tr>
<tr>
<td>Object Type</td>
<td>Permissions</td>
<td>Information Link</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>All Rulesets (BLACK List Rulesets and NXDOMAIN Rulesets)</td>
<td>For more information, see Administrative Permissions for DHCP Resources.</td>
<td></td>
</tr>
<tr>
<td>All DNS64 Synthesis Groups</td>
<td>For more information, see Administrative Permissions for DNS64 Synthesis Groups.</td>
<td></td>
</tr>
<tr>
<td>All Response Policy Zones</td>
<td>For more information, see Administrative Permissions for Zones and License Requirements and Admin Permissions.</td>
<td></td>
</tr>
<tr>
<td>All Response Policy Rules</td>
<td>For more information, see Administrative Permissions for Zones and License Requirements and Admin Permissions.</td>
<td></td>
</tr>
<tr>
<td>All DTC Objects (LBDN Records, LBDNs, Pools, Servers, Monitors, Certificates, GeoIP and Topologies)</td>
<td>For more information, see License Requirements and Admin Permissions.</td>
<td></td>
</tr>
<tr>
<td>Adding a blank A/AAAA record</td>
<td>For more information, see Administrative Permissions for Common Tasks.</td>
<td></td>
</tr>
<tr>
<td>File Distribution Permissions</td>
<td>Grid File Distribution Permissions</td>
<td>For more information, see Administrative Permissions for File Distribution Services.</td>
</tr>
<tr>
<td>Grid Permissions</td>
<td>All Members</td>
<td>For more information, see Administrative Permissions for Common Tasks.</td>
</tr>
<tr>
<td>Network Discovery</td>
<td>For more information, see Administrative Permissions for Network Discovery.</td>
<td></td>
</tr>
<tr>
<td>Schedule Tasks</td>
<td>For more information, see Administrative Permissions for Scheduling Tasks.</td>
<td></td>
</tr>
<tr>
<td>CSV Import</td>
<td>For more information, see Administrative Permissions for CSV Import.</td>
<td></td>
</tr>
<tr>
<td>All Microsoft Servers</td>
<td>For more information, see Administrative Permissions for Microsoft Servers.</td>
<td></td>
</tr>
<tr>
<td>All Dashboard Tasks</td>
<td>For more information, see Administrative Permissions for Dashboard Tasks.</td>
<td></td>
</tr>
<tr>
<td>All Kerberos keys</td>
<td>For more information, see Admin Permissions for Configuring GSS-TSIG keys.</td>
<td></td>
</tr>
<tr>
<td>All Active Directory Domains</td>
<td>For more information, see Managing Active Directory Sites.</td>
<td></td>
</tr>
<tr>
<td>IPAM Permissions</td>
<td>All Network Views</td>
<td>For more information, see Administrative Permissions for Common Tasks.</td>
</tr>
<tr>
<td>All IPv4 Networks</td>
<td>For more information, see Administrative Permissions for IPv4 and IPv6 Networks.</td>
<td></td>
</tr>
<tr>
<td>All IPv6 Networks</td>
<td>For more information, see Administrative Permissions for IPv4 and IPv6 Networks.</td>
<td></td>
</tr>
<tr>
<td>All Hosts</td>
<td>For more information, see Administrative Permissions for Hosts.</td>
<td></td>
</tr>
<tr>
<td>All IPv4 Host Addresses</td>
<td>For more information, see Administrative Permissions for DNS Resources with Associated IP addresses in Networks and Ranges.</td>
<td></td>
</tr>
<tr>
<td>All IPv6 Host Addresses</td>
<td>For more information, see Administrative Permissions for DNS Resources with Associated IP addresses in Networks and Ranges.</td>
<td></td>
</tr>
<tr>
<td>Port Control</td>
<td>For more information, see Administrative Permissions for Network Discovery.</td>
<td></td>
</tr>
<tr>
<td>Security Permissions</td>
<td>Grid Security Permissions</td>
<td>For more information, see Administrative Permissions.</td>
</tr>
<tr>
<td>Reporting Permissions</td>
<td>Grid Reporting Permissions</td>
<td>For more information, see Administrative Permissions for Common Tasks.</td>
</tr>
<tr>
<td>Reporting Dashboard</td>
<td>For more information, see Administrative Permissions for Reporting.</td>
<td></td>
</tr>
<tr>
<td>Reporting Search</td>
<td>For more information, see Administrative Permissions for Reporting.</td>
<td></td>
</tr>
</tbody>
</table>

### Defining Object Permissions

You can add permissions to specific objects for selected admin groups or roles. When you add permissions to objects, you can select multiple objects with the same or different object types. When you select multiple objects with the same object type, you can apply permissions to the selected objects as well as the sub object types that are contained in the selected objects. As described in Figure 4.2, when you select five DNS...
forward-mapping authoritative zones, the appliance displays the object type “AuthZone” for all the zones. Since all five DNS zones are of the same object type, you can also apply permissions to all the resource records in these zones. The appliance displays the resources in the resource section of the Create Object Permissions editor. You can choose one or more of the resources to which you want to apply permissions.

In Cloud Network Automation, admin groups and admin users who have cloud API access have full permissions to delegated. However, you must specifically assign permissions for objects that have not been delegated in order for any admin groups or admin users to gain permission to these objects. Therefore, an admin group that has access to the cloud API would have full permissions to all delegated objects but limited permissions to non-delegated objects.

For information about how to allow cloud API access to an admin group, see Creating Limited-Access Admin Groups. For information about guidelines for authority delegation, see About Authority Delegation. Figure 4.2 Selecting Multiple Objects with the Same Object Type

When you select multiple objects with more than one object type, you can add permissions to the selected objects as well as to the sub object types that are common among the selected objects. For example, when you select three DNS forward-mapping authoritative zones and two DNS IPv4 reverse-mapping authoritative zones as illustrated in Figure 4.3, you can apply permissions to all the five DNS zones as well as to the CNAME, DNAME, and host records in these zones because CNAME, DNAME, and host records are the common sub object types in these zones.

Figure 4.3 Multiple Objects with Common Sub Object Types
When you select three DNS forward-mapping authoritative zones and two IPv4 reverse-mapping authoritative zones, you can apply object permissions to all the DNS zones as well as the CNAME, DNAME and Host records in these DNS zones.

To define object permissions for an admin group or role:

1. For an admin group: From the Administration tab, select the Administrators tab -> Permissions tab -> admin_group in the Groups table, and then click the Add icon -> Object Permissions from the Create New Permission area or select Add -> Object Permissions from the Toolbar.
   or
   For an admin role: From the Administration tab, select the Administrators tab -> Permissions tab -> admin_role in the Roles table, and then click Add icon -> Object Permissions from the Create New Permission area or select Add -> Object Permissions from the Toolbar.
2. Grid Manager displays the Create Object Permissions wizard. For an admin group, the appliance displays the selected group in the Group field. For an admin role, the appliance displays the selected admin role in the Role field. You can also select a different group or role from the drop-down list.
3. Click Select Object(s). Grid Manager displays the Object Selector dialog box.
4. In the Object Selector dialog box, complete the following:
   - Enter a value or partial value of an object in the first field. This field is not case-sensitive. For example, if the object to which you want to define permissions contains "Infoblox", enter Infoblox here.
   - Select the object type for which you are searching in the Type drop-down list. By default, the appliance searches all object types.
   - In the operator drop-down list, select an operator for the filter criteria. Depending on what you select in the first filter field, this list displays the relevant operators for the selection.
   - In the value field, enter or select the attribute value for the first filter field. Depending on what you select for the first two filter fields, you can either enter a value or select a value from a drop-down list.
5. Click Search. The appliance lists all matching objects in the table. You can select multiple object types by clicking the Add icon to add more filter criteria. You can also click Reset to clear all entries.
6. Select the check boxes of the objects to which you are defining permissions, and then click the Select icon.
7. In the Create Object Permissions wizard, do the following:
   - Object: Displays the name of the selected object. When you select multiple objects, the appliance displays Multiple here. Mouse over to the information icon to view the list of objects to which you are defining permissions.
   - Object Type: Displays the object type of the selected object. When you select more than one object type, the appliance displays Multiple here.
   - Resource: Displays the selected objects. When you select more than one object type, the appliance displays Multiple Selected Objects here. Mouse over to the information icon to view the list of objects to which you are defining permissions. Grant the resources an appropriate permission: Read/Write, Read Only, or Deny.
8. Save the configuration and click Restart if it appears at the top of the screen.

Grid Manager displays a warning message when the permissions you define here overlap with other permissions in the system. Click See Conflicts to view the overlapping permissions in the Permissions Conflict dialog box. For information, see Applying Permissions and Managing Overlaps. You can also set permissions for specific objects from the objects themselves. For example, to define permissions for a particular Grid member, navigate to that Grid member and define its permissions.

To define the permissions of a specific object:

1. Navigate to the object. For example, to define permissions for a particular network, from the Data Management tab, select the IPAM tab -> network check box, and then click the Edit icon.
2. In the editor, select the Permissions tab, and then do one of the following:
   - Click the Add icon to add permission to the object. In the Admin Group/Role Selector dialog box, select an admin group or role to which you want to assign the permission, and then click the Select icon.
   - Modify the permission and resource type of a selected admin group or role.
   - Select an admin group or role and click the Delete icon to delete it.
3. Save the configuration and click Restart if it appears at the top of the screen.

---

### Defining DNS and DHCP Permissions on Grid Members

You can restrict certain admin groups or roles to perform specific DNS and DHCP tasks on specific Grid members by assigning the correct global and object permissions. You can use this feature to separate the DNS and DHCP administration on different Grid members. For example, you can create an admin group or role that can only create, modify, and delete DHCP ranges in a specific network on a specific member in the Grid. This admin group or role is restricted to the specified tasks on the selected Grid member. It cannot perform other DNS or DHCP tasks on this member, and it cannot perform the specified tasks on other Grid members.

For example, you can define permissions that allow admins to create, modify, and delete DHCP ranges in network 10.0.0.0/8 on Grid member "sales.infoblox.com" by granting read/write object permissions to all DHCP ranges, network 10.0.0.0/8, and member DHCP on sales.infoblox.com. Admins with these permissions can only add, modify, and delete DHCP ranges in network 10.0.0.0/8 on Grid member sales.infoblox.com. They cannot perform other DHCP or DNS tasks on the member, and they cannot perform these tasks on other Grid members.

For information about required permissions for specific DNS and DHCP tasks, see Administrative Permissions for Common Tasks. You can define the following DNS and DHCP permissions for an admin group or role:

- Grid DNS or Grid DHCP: Admins with read/write permissions can manage any DNS or DHCP resources on any Grid members. They can also modify Grid DNS or Grid DHCP properties and any member DNS and member DHCP properties. Admins with read-only permissions can only view DNS or DHCP resources. They cannot modify any DNS or DHCP resources or restart related services.
- Member DNS or Member DHCP: Admins with read/write permissions can perform the defined DNS or DHCP tasks only on the specified Grid member, not any other members. They can also modify DNS or DHCP properties on the specified member. Admins with read-only permission cannot assign the Grid member to any DNS or DHCP resources.
- Restart DNS or Restart DHCP on member: Admins with read/write permissions can restart the DNS or DHCP service on the specified Grid member, not any other members. However, they cannot modify DNS or DHCP properties on the member. They can assign the specified Grid member to any DNS or DHCP resources, but they cannot assign any other Grid members to DNS or DHCP resources.

To specify member DNS and DHCP permissions, define DNS or DHCP permissions at the global or level for an admin group or admin role, as described in Defining Global Permissions and Defining Object Permissions. Ensure that you include the Grid member object to which you want to restrict DNS or DHCP administration. You can assign valid permissions to administrators to manage kerberos keys. For more information, see Admin Permissions for Configuring GSS-TSIG keys.

You can also control whether the admins can modify DNS or DHCP properties on a member, as described in Modifying Permissions on a Grid Member.

---

### Modifying Permissions on a Grid Member

Admins can perform different tasks on a Grid member based on the permissions they have. Table 4.3 outlines the permissions and the tasks.
admins can perform on a Grid member:

**Table 4.3 Member Permissions and Tasks**

<table>
<thead>
<tr>
<th>Grid Member</th>
<th>Member DNS or DHCP Properties</th>
<th>Restart DNS or DHCP on Grid Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read/Write</td>
<td>• Modify member properties</td>
<td>• Restart member DNS or DHCP</td>
</tr>
<tr>
<td></td>
<td>• Restart, reboot, and shutdown member</td>
<td>service</td>
</tr>
<tr>
<td></td>
<td>• Modify member DNS and DHCP properties</td>
<td>• Assign and un-assign member to DNS and DHCP objects</td>
</tr>
<tr>
<td></td>
<td>• Restart member DNS and DHCP services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Assign and un-assign member to DNS and DHCP objects</td>
<td></td>
</tr>
<tr>
<td>Read-only</td>
<td>• View member DNS and DHCP properties</td>
<td>• View member DNS or DHCP properties</td>
</tr>
<tr>
<td>Deny</td>
<td>• Cannot modify member, DNS, and DHCP properties</td>
<td>• Cannot modify member, DNS, and DHCP properties</td>
</tr>
<tr>
<td></td>
<td>• Cannot restart related services</td>
<td>• Cannot restart related services</td>
</tr>
<tr>
<td></td>
<td>• Cannot assign member to DNS and DHCP objects</td>
<td>• Cannot assign member to DNS and DHCP objects</td>
</tr>
<tr>
<td></td>
<td>Restart member DNS or DHCP service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assign and un-assign member to DNS or DHCP objects</td>
<td></td>
</tr>
</tbody>
</table>

After you add permissions to an admin group or role for a specific Grid member, you can modify the member permissions and resources. Note that when you modify the member permissions and resources, the appliance updates the permissions of the admin group or role accordingly.

To modify Grid member permissions:

1. From the **Data Management** tab, select the **DHCP** or **DNS** tab -> **Members** tab -> **Grid_member**, and then click the **Edit** icon.
2. In the **Member DHCP Properties** or **Member DNS Properties** editor, select the **Permissions** tab.
3. Click a permission in the Permissions table, select a different permission from the **Permissions** drop-down list or select a different resource from the **Resources** drop-down list. Note that when you select **Restart DNS** or **Restart DHCP**, the admins with this permission can only restart the DNS or DHCP service on the selected member. They cannot modify DNS or DHCP properties of this member.
4. Save the configuration. Note that the appliance automatically updates the permissions of the corresponding admin group or role in the **Administration** tab.

### Applying Permissions and Managing Overlaps

When an admin tries to access an object, the appliance checks the permissions of the group to which the admin belongs. Because permissions at more specific levels override those set at a higher level, the appliance checks object permissions hierarchically—from the most to the least specific. In addition, if the admin group has permissions assigned directly to it and permissions inherited from its assigned roles, the appliance checks the permissions in the following order:

1. Permissions assigned directly to the admin group.
2. Permissions inherited from admin roles in the order they are listed in the **Roles** tab of the **Admin Group** editor.

For example, an admin from the DNS1 admin group tries to access the a1.test.com A record in the test.com zone in the Infoblox default view. The appliance first checks if the DNS1 admin group has a permission defined for the a1.test.com A record. If there is none, then the appliance checks the roles assigned to DNS1. If there is no permission defined for the a1.test.com A record, the appliance continues checking for permissions in the order listed in **Table 4.4**. The appliance uses the first permission it finds.

### Table 4.4 Permission Checking

<table>
<thead>
<tr>
<th>The appliance checks object permissions from the most to the least specific, as listed.</th>
<th>For each object, the appliance checks permissions in the order listed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. a1.test.com A record</td>
<td>a. DNS1 admin group</td>
</tr>
<tr>
<td>2. A records in test.com</td>
<td>b. Role 1, Role 2, Role 3...</td>
</tr>
<tr>
<td>3. test.com</td>
<td></td>
</tr>
<tr>
<td>4. All zones in the default view</td>
<td></td>
</tr>
<tr>
<td>5. Default view</td>
<td></td>
</tr>
<tr>
<td>6. All A records</td>
<td></td>
</tr>
<tr>
<td>7. All zones</td>
<td></td>
</tr>
<tr>
<td>8. All DNS views</td>
<td></td>
</tr>
</tbody>
</table>

An admin group that is assigned multiple roles and permissions can have overlaps among the different permissions. As stated earlier, the appliance uses the first permission it finds and ignores the others. For example, as shown in **Table 4.5**, if an admin group has read/write permission to all A records in the test.com zone and a role assigned to it is denied permission to test.com, the appliance provides read/write access to A records in the test.com zone, but denies access to the test.com zone and all its other resource records.

### Table 4.5 Directly-Assigned Permissions and Roles

<table>
<thead>
<tr>
<th>Permission assigned to the admin group</th>
<th>Read/Write to all A records in the test.com zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission inherited from an admin role</td>
<td>Deny to the test.com zone</td>
</tr>
</tbody>
</table>
Effective permissions  | Deny to the test.com zone  
| Read/Write to all A records in test.com zone  
| Deny to all other resource records in test.com zone

If the group has multiple roles, the appliance applies the permissions in the order the roles are listed. If there are overlaps in the permissions among the roles, the appliance uses the permission from the role that is listed first. For example, as shown in Table 4.6, the first role assigned to the admin group has read-only permission to all A records in the test.com zone and the second role has read/write permission to the same records. The appliance applies the permission from the first admin role.

Table 4.6 Multiple Roles

| Role 1 permission | Read-only to all A records in the test.com zone |
| Role 2 permission | Read/Write to all A records in test.com zone  
| Read/Write to all MX records in test.com zone |
| Effective permissions | Deny to the test.com zone  
| Read-only to all A records in the test.com zone  
| Read/Write to all MX records in test.com zone |

You can check for overlapped permissions when you add permissions to roles and to admin groups, and when you assign roles to an admin group. When you create a permission that overlaps with existing permissions, Grid Manager displays a warning message and the SeeConflicts link on which you click to view the overlapped permissions. For information, see Viewing Overlapping Permissions. You can also use the quick filter Overlaps to filter overlapped permissions, the appliance lists permissions that overlap with other permissions. If you want to change the permission the appliance uses, you must change the order in which the roles are listed or change the permissions that are directly assigned to the admin group. For information, see Creating Limited-Access Admin Groups.

Viewing Overlapping Permissions

When you click See Conflicts to view overlapping permissions, Grid Manager displays the following information in the Permission Overlap dialog box:

1. **Resource**: The name of the object or resource.
2. **Type**: The object type.
3. **Permission**: The permission granted. This can be Read/Write, Read-Only, or Deny.
4. **Inherited From**: Indicates the source from which the permission is inherited.
5. **Conflict Status**: Indicates whether the permission is being used or ignored. In a permission overlap, the group permission always overrides the role permission if both permissions are set at the same level (global or object). However, if the permissions are set at different levels, the permission at a more specific level overrides that set at a higher level.
6. **Role/Group Name**: The name of the admin group or admin role.

You can click the arrow key next to the resource to view the permission that is being ignored in the overlap.

Managing Permissions

After you define permissions for an admin group and role, you can do the following:

- View the permissions, as described in Viewing Permissions.
- Modify the permissions, as described in Modifying Permissions
- Delete the permission, as described in Deleting Permissions.

Viewing Permissions

Only superusers can view the permissions of all admin groups. To view the permissions of an admin group or role:

1. From the Administration tab, select the Administrators tab -> Permissions tab.
2. For an admin group: Select an admin group in the Groups table.
   or
   For an admin role: Select an admin role in the Roles table.
3. Grid Manager displays the following information in the Permissions table:
   - **Group/Role**: The name of the admin group or role.
   - **Permission Type**: The type of permissions. This can be Administration Permissions, Analytics Permissions, Cloud Permissions, Named ACL Permissions, DHCP Permissions, DNS Permissions, File Distribution Permissions, Grid Permissions, IPAM Permissions, Reporting Permissions, or Security Permissions.
   - **Resource**: The name of the object. For example, this field displays All Hosts if you have defined permissions for all the hosts in the Grid.
   - **Resource Type**: The object type. For example, this can be Host, PTR record, or Shared Network.
   - **Permission**: The defined permission for the resource.
When you click **Show All** for Admins, Groups, and Roles, Grid Manager displays all the admin accounts, admin groups, and admin roles in their respective tables.

**Filtering the List of Permissions**

You can filter the permissions you want to view by selecting one of the following from the quick filter menu:

- **Effective Permissions**: Select to view only the permissions that the appliance is using for this group. The permissions that were ignored due to overlaps are not listed in this view.
- **Overlaps**: Select to view only the overlapped permissions.
- **All Configured Permissions**: Select to view all permissions.

**Modifying Permissions**

You can modify the permissions of user-defined admin roles and admin groups. You cannot modify the permissions of system-defined admin roles. When you change the permissions of a role that has been assigned to multiple admin groups, the appliance automatically applies the change to the role in all admin groups to which it is assigned.

To modify the existing permissions of a role or an admin group:

1. From the **Administration** tab, select the **Administrators** tab ➔ **Permissions** tab.
2. For an admin group: Select an admin group in the Groups table. or
3. For an admin role: Select an admin role in the Roles table.
4. In the Permissions table, select the resource that you want to modify, and then click the **Edit** icon.
5. In the **Manage Global Permissions** or **Create Object permissions** editor, select the new permission: **Read/Write**, **Read-Only** or **Deny** for the resource.
6. Save the configuration and click **Restart** if it appears at the top of the screen.

**Deleting Permissions**

You can remove permissions from user-defined admin roles and admin groups. You cannot remove permissions from system-defined admin roles. When you remove permissions from a role, they are removed from the role in all admin groups to which the role is assigned. You can remove a permission from a group as long as it is not inherited from a role. You cannot remove permissions that are inherited from a role.

To delete a permission:

1. From the **Administration** tab, select the **Administrators** tab ➔ **Permissions** tab.
2. For an admin group: Select an admin group in the Groups table. or
   - For an admin role: Select an admin role in the Roles table.
3. In the Permissions table, select the resource that you want to modify, and then click the **Delete** icon.
4. In the **Delete Permission Confirmation** dialog box, click **Yes**.

**Authenticating Administrators**

The NIOS appliance supports the following authentication methods: local database, RADIUS, Active Directory, LDAP, and TACACS+. The appliance can use any combination of these authentication methods. It authenticates admins against its local database by default. Therefore, if you want to use local authentication only, you must configure the admin groups and add the local admin accounts, as described in **Creating Local Admins**.

Depending on where admin user credentials are stored, you can configure the NIOS appliance to authenticate admins locally or remotely. When you configure the authentication type as "local," NIOS authenticates admins against its local database. When you configure the authentication type as "remote," NIOS authenticates admins whose user credentials are stored remotely on authentication servers, such as RADIUS servers, AD domain controllers, LDAP servers, or TACACS+ servers.

Note the following when you configure remote authentication type for local admins:

- You cannot define two local admins that have the same name and belong to different authentication server groups.
- Only superusers can modify the authentication type for other admin accounts.
- At least one superuser account must use the remote authentication type.

To authenticate admins using RADIUS, Active Directory, TACACS+, or LDAP in addition to local authentication, you must define those services on the appliance and define the admin authentication policy. For information, see **About Remote Admins**.

NIOS also supports two-factor authentication where it authenticates the following:

1. Administrators through the admin authentication policy.
2. Admin client certificates through the certificate authentication service.

For more information about two-factor authentication and how to configure it, see **Defining the Authentication Policy**.

**Note**: If you are using remote authentication, you must always have at least one local admin in a local admin group to ensure connectivity to the NIOS appliance in case the remote servers become unreachable.

**Creating Local Admins**

When you create an admin account, you must specify the authentication type, name, password, and admin group of the administrator. You can also control in which time zone the appliance displays the time in the audit log and the DHCP and IPAM tabs of Grid Manager, such as the **DHCP Lease History** and **DHCP Leases** panels. The appliance can use the time zone that it automatically detects from the management system that the
To define the password requirements for local admins:

1. Log in as a superuser.
2. From the Administration tab, select the Administrators tab -> Admins tab, and then click the Add icon.
   or
   From the Administration tab, select the Administrators tab -> Groups tab -> admin_group, and then click the Add icon.
3. In the Add Administrator wizard, complete the following:
   - **Authentication Type**: You can select either **Local** or **Remote** from the drop-down list. The default is **Local**. When you select **Local**, NIOS authenticates admins against its local database. When you select **Remote**, NIOS authenticates admins based on the user credentials stored remotely on authentication servers, such as RADIUS servers, AD domain controllers, LDAP servers, or TACACS+ servers.
     - **Local**: The following fields are displayed when you select **Local** authentication type. Enter the following:
       - **Login**: Enter a name for the administrator. This is the username that the administrator uses to log in to the appliance. This username is stored in the NIOS local database.
       - **Password**: Enter a password for the administrator. This is the password that the administrator uses to log in to the appliance. This password is stored in the NIOS local database.
       - **Confirm Password**: Enter the same password.
     - **Remote**: The following field is displayed when you select **Remote** authentication type. Enter the following login credentials:
       - **Login**: Enter a name for the administrator that is stored in the database of the remote server. This is the username that the administrator uses to log in to the appliance.

**Note**: You cannot configure the **Remote** authentication type for NIOS admin users who belong to the **fireeye-group** admin groups.

   - **Email Address**: Enter the email address for this administrator. The appliance uses this email address to send scheduling notifications.
   - **Admin Group**: Click **Select** to specify an admin group. If there are multiple admin groups, Grid Manager displays the Admin Group Selector dialog box from which you can select one. An admin can belong to only one admin group at a time.

NIOS appliance creates a new group, **fireeye-group**, when you add the first FireEye zone. The FireEye admin group is read-only and you cannot assign permissions to it. Select **fireeye-group** for the admin group and add users to this group. For more information, see About FireEye Integrated RPZs.

**Note**: You cannot add a NIOS admin user that uses the Remote authentication type to the **fireeye-group** admin group.

   - **Comment**: Enter useful information about the administrator.
   - **Disable**: Select this check box to retain an inactive profile for this administrator in the configuration. For example, you might want to define a profile for a recently hired administrator who has not yet started work. Then when he or she does start, you simply need to clear this check box to activate the profile.

4. Optionally, click **Next** to add extensible attributes to the admin account. For information, see About Extensible Attributes.
5. Save the configuration and click **Restart** if it appears at the top of the screen.

### Managing Passwords

Superusers can define requirements for the passwords of local admins according to your organization’s policies. In addition to specifying the minimum password length, you can define rules that specify the character types that are allowed in the password. You can also specify whether passwords expire, their duration, and when reminders are sent to the users. Additionally, you can require admins to change their passwords when they first log in or after their passwords are reset.

You set the requirements at the Grid level, so they apply to all local admins who log in to the Grid. The requirements that you define appear in the User Profile of all local admins and when users are required to change their password.

To define the password requirements for local admins:

1. From the **Grid** tab, select the **Grid Manager** tab.
2. Expand the Toolbar and select **Grid Properties -> Edit**.
3. In the **Grid Properties** editor, select the **Password** tab and complete the following:
   - **Minimum Password Length**: Specify the minimum number of characters that are required in a password.
   - **Password Complexity**: You can set up some requirements around how users compose a password by specifying the category and the number of characters and/or symbols the password must contain. The default is 0 for all categories, which means the password is not required to contain those characters. Specify the minimum number of characters the password must contain for the following:
     - lowercase characters [a-z]
     - uppercase characters [A-Z]
     - numeric characters [0-9]
     - symbol characters. Allowed characters are: ! @ # $ % ^ _ * ( )
     - character changes from previous passwords. To discourage users from reusing previous passwords, you can require a minimum change of characters from previous passwords.
• **Password must expire:** Select this check box to enable passwords to expire after a specified period. Specify the duration of each password and the number of days before the expiration that the appliance sends a reminder.
• **Force password change at next login:** Select this check box to force all new users to change their passwords when they first log in and to force existing users whose passwords were just reset to change their passwords.

**Note:** The "force password change at next login" feature does not apply to admin users in the fireeye-group. These users will not be prompted to change their passwords at the next login. Their original passwords continue to work. For information about FireEye integrated RPZs, see About FireEye Integrated RPZs.

4. Click **Save & Close.**

### Modifying and Deleting Admin Accounts

You can modify and delete admin accounts that you create, but you can only partially modify the default superuser account "admin"—and only when you are logged in as a superuser account. Furthermore, because there must always be a superuser account on the appliance, you can only remove the default "admin" account after you create another superuser account.

To modify an admin account:

1. From the **Administration** tab, select the **Administrators** tab -> **Admins** tab -> **admin_account** check box, and then click the Edit icon. or
   From the **Administration** tab, select the **Administrators** tab -> **Groups** tab -> **admin_group** -> **admin_account** check box, and then click the Edit icon.
2. The **Administrator** editor provides the following tabs from which you can modify data:
   - **General:** In the **General Basic** tab, modify data of the admin account as described in Creating Local Admins. In the **General Advanced** tab, complete the following:
     - **Time Zone:** Select a time zone from the drop-down list if you want to specify the time zone for the administrator. By default, the appliance automatically detects the time zone from the management system that the administrator uses to connect to the appliance. The appliance uses this time zone when it displays the timestamps for relevant data.
     - **Enable Certificate Authentication:** Select the check box to enable the certificate authentication service. You must also specify the serial number of the client certificate and associate a CA certificate that signs the client certificate. For more information, see Enabling Certificate Authentication Service for a User.
   - **Extensible Attributes:** Add and delete extensible attributes that are associated with the admin account. You can also modify the values of the extensible attributes. For information, see About Extensible Attributes.
3. Save the configuration and click **Restart** if it appears at the top of the screen.

To delete an admin account:

1. From the **Administration** tab, select the **Administrators** tab -> **Admins** tab -> **admin_account** check box, and then click the Delete icon. or
   From the **Administration** tab, select the **Administrators** tab -> **Groups** tab -> **admin_group** -> **admin_account** check box, and then click the Delete icon.
2. In the **Delete Confirmation** dialog box, click **Yes.**

### About Remote Admins

NIOS can authenticate admins whose user credentials are stored remotely on RADIUS servers, AD domain controllers, LDAP servers, or TACACS+ servers. You can configure authentication server groups for each type of server to which NIOS sends authentication requests. For example, you can create a server group for RADIUS servers and another server group for AD domain controllers. Then in the admin authentication policy, you can list which authentication server groups to use and in what order.

In addition, if admin groups are configured on the remote authentication server, you can configure admin groups with the same names on the NIOS appliance and list them in the authentication policy as well. Then if the remote authentication server provides the admin group name while authenticating an admin, NIOS can automatically assign the admin to the matching admin group specified in the authentication policy. You can also create a default admin group for all admins that are authenticated through a remote authentication service.

4820254 illustrates the authentication and authorization process for remote admins. In the example, two authentication server groups are configured—a RADIUS server group and an AD server group. When an admin logs in with a user name and password, the appliance uses the first service listed in the admin policy to authenticate the admin. If authentication fails, the appliance tries the next service listed, and so on. It tries each service on the list until it is successful or all services fail. If all services fail, then the appliance denies access and generates an error message in syslog.

If authentication succeeds, the NIOS appliance tries to match the admin group names in the admin policy to any groups received from the remote server. If it finds a match, the NIOS appliance applies the privileges of that group to the admin and allows access. If the appliance does not find a match, then it applies the privileges of the default group. If no default group is defined, then the appliance denies access.

*Figure 4.4 Authenticating Remote Admins*
Only superusers can perform the following tasks to configure NIOS to authenticate admins using remote authentication servers:

- Configure the authentication server groups. You can create multiple RADIUS, LDAP, and AD server groups, and certificate authentication services, but only one TACACS+ server group.
  - For information about RADIUS authentication, see Authenticating Admins Using RADIUS.
  - For information about AD authentication, see Authenticating Admins Using Active Directory.
  - For information about TACACS+ authentication, see Authenticating Admin Accounts Using TACACS+.
  - For information about LDAP authentication, see Authenticating Admins Using LDAP.
  - For information about the certificate authentication service, see Authenticating Admins Using Two-Factor Authentication.
- Configure admin groups with names that match those on the remote server. For information about admin groups, see About Admin Groups.
- Configure the admin policy, as described in Defining the Authentication Policy.

Note: Infoblox strongly recommends that even if you are using remote authentication, you always have at least one local admin in a local admin group to ensure connectivity to the appliance in case the remote servers become unreachable. Also, when you delete an authentication server group, the appliance removes it from the system. Deleted authentication server groups are not moved to the Recycle Bin. Once deleted, the authentication server groups no longer exist in the system.

When remote authentication is successful, the appliance creates a remote admin user object in the NIOS database, which stores user preferences such as time zone, table size, and active Dashboard widgets for the remote user. If the remote user does not log in to the appliance for more than 180 days, the appliance removes the corresponding admin user object from the database. Although the remote user can still log in to the appliance, user preferences are lost. The Grid Master performs this cleanup action once a day.

You can also authenticate users based on X.509 client certificates. You can configure NIOS to authenticate these admins through the two-factor authentication method. For more information about two-factor authentication and how to configure it, see Defining the Authentication Policy.

**Authenticating Admins Using RADIUS**

RADIUS provides authentication, accounting, and authorization functions. The NIOS appliance supports authentication using the following RADIUS servers: FreeRADIUS, Microsoft, Cisco, and Funk.

When NIOS authenticates administrators against RADIUS servers, NIOS acts similarly to a network access server (NAS), which is a RADIUS client that sends authentication and accounting requests to a RADIUS server. Figure 4.5 illustrates the RADIUS authentication process.
When you configure the NIOS appliance to authenticate admins against a RADIUS server group, you must specify the authentication protocol of each RADIUS server, which can be either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol).

PAP tries to establish the identity of a host using a two-way handshake. The client sends the user name and password in clear text to the NIOS appliance. The appliance uses a shared secret to encrypt the password and sends it to the RADIUS server in an Access-Request packet. The RADIUS server uses the shared secret to decrypt the password. If the decrypted password matches a password in its database, the user is successfully authenticated and allowed to log in.

With CHAP, when the client tries to log in, it sends its user name and password to the NIOS appliance. The appliance then creates an MD5 hash of the password together with a random number that the appliance generates. It then sends the random number, user name, and hash to the RADIUS server in an Access-Request package. The RADIUS server takes the password that matches the user name from its database and creates its own MD5 hash of the password and random number that it received. If the hash that the RADIUS server generates matches the hash that it received from the appliance, then the user is successfully authenticated and allowed to log in.

You can configure one of the following modes to send the authentication request to the RADIUS server:

- **Ordered**: In this mode, the authentication request is sent to the first server in the list. The authentication request is sent to the next server only when the first server is out of service or unavailable.
- **Round Robin**: In this mode, the first authentication request is sent to a server chosen randomly in a group. If there is no response from the server, continued attempts are performed sequentially until it selects the last server in the list. Then it starts with the first server in the list and continues the selection process until all the servers have been attempted.

**Accounting Activities Using RADIUS**

You can enable the accounting feature on the RADIUS server to track whether an administrator has initiated a session. After an administrator successfully logs in, the appliance sends an Accounting-Start packet to the RADIUS server.

**Configuring Remote RADIUS Servers**

For NIOS to communicate with a RADIUS server, you must also set up the remote RADIUS server to communicate with the NIOS appliance.

**Note**: If you have two Infoblox appliances in an HA pair, enter both the members of the HA pair as separate access appliances and use the LAN or MGMT IP address of both appliances (not the VIP address), if configured.

Depending on your particular RADIUS server, you can configure the following RADIUS server options to enable communication with the NIOS appliance:

- Authentication Port
- Accounting Port
- Domain Name/IP Address of the NIOS appliance
- Shared Secret Password
- Vendor Types

**Configuring Admin Groups on the Remote RADIUS Server**

Infoblox supports admin accounts on one or more RADIUS servers.
On the remote RADIUS server, do the following to set up admins and associate them with an admin group:

- Import Infoblox VSAs (vendor-specific attributes) to the dictionary file on the RADIUS server
- For third-party RADIUS servers, import the Infoblox vendor file (the Infoblox vendor ID is 7779)
- Define the admin group
- Associate one or more remote admin accounts with the admin group
- Add and activate a policy for the admin accounts, but do not associate the policy with a policy group that contains an infoblox-group-info attribute.

Refer to the documentation for your RADIUS server for more information.

**Configuring RADIUS Authentication**

To configure NIOS to use one or more RADIUS server groups to authenticate administrators, you must do the following:

- Configure at least one RADIUS authentication server group. For more information, see Configuring a RADIUS Authentication Server Group.
- Define admin groups for the admins that are authenticated by the RADIUS servers and specify their privileges and settings. The group names in NIOS must match the admin group names on the RADIUS server. See About Admin Groups for information about defining admin groups.
- In the authentication policy, add the RADIUS server groups and the admin groups that match those on the RADIUS server. You can also designate an admin group as the default group for remote admins. NIOS assigns admins to this group when it does not find a matching group for a remote admin. See Defining the Authentication Policy for more information about configuring the policy.

**Configuring a RADIUS Authentication Server Group**

You can add multiple RADIUS servers to the group for redundancy. When you do, the appliance tries to connect to the first RADIUS server on the list and if the server does not respond within the maximum retransmission limit, then it tries the next RADIUS server on the list. NIOS tries to connect to each RADIUS server in the order the servers are listed. If it does not receive a response within the configured timeout period and has tried to connect the specified retry value, then it tries the next RADIUS server on the list. It logs an error to syslog when it fails to connect to any of the servers in the group.

After you add a RADIUS server to the NIOS appliance, you can validate the configuration. The appliance uses a pre-defined username and password when it tests the connection to the RADIUS server. The pre-defined user name is "Infoblox_test_user" and the password is "Infoblox_test_password". Do not use these as your administrator username and password.

To configure a RADIUS authentication server group:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Click the Add icon in the RADIUS Services subtab.
3. In the Add RADIUS Authentication Service wizard, complete the following:
   - **Name**: Enter the name of the server group.
   - **RADIUS Servers**: Click the Add icon and enter the following:
     - **Server Name or IP Address**: Enter the FQDN or the IP address of the RADIUS server that is used for authentication.
     - **Comment**: Enter additional information about the RADIUS server.
     - **Authentication Port**: The destination port on the RADIUS server. The default is 1812. This field is required only if you do not enable accounting on the RADIUS server. This field is not required if you enable accounting to configure an accounting-only RADIUS server.
     - **Authentication Type**: Select either PAP or CHAP from the drop-down list. The default is PAP.
     - **Shared Secret**: Enter the shared secret that the NIOS appliance and the RADIUS server use to encrypt and decrypt their messages. This shared secret is a value that is known only to the NIOS appliance and the RADIUS server.
     - **Enable Accounting**: Select this to enable RADIUS accounting for the server so you can track an administrator’s activities during a session. When you enable accounting, you must enter a valid port number in the Accounting Port field.
     - **Accounting Port**: The destination port on the RADIUS server. The default is 1813.
   - **Connect through Management Interface**: Select this so that the NIOS appliance uses the MGMT port for administrator authentication communications with just this RADIUS server.
   - **Disable server**: Select this to disable the RADIUS server if, for example, the connection to the server is down and you want to stop the NIOS appliance from trying to connect to this server.
   - **Click Test** to test the configuration. If the NIOS appliance connects to the RADIUS server using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the RADIUS server, the appliance displays a message indicating an error in the configuration.
   - **Click Add** to add the server to the list.

When you add multiple RADIUS servers, the appliance lists the servers in the order you added them. This list also determines the order in which the NIOS appliance attempts to contact a RADIUS server. You can move a server up or down the list by selecting it and clicking the up or down arrow.

You can also delete a RADIUS server by selecting it and clicking the Delete icon.

- **Authentication**: Optionally, modify the authentication settings. These settings apply to all RADIUS servers that you configure on the NIOS appliance.
- **Timeout(s)**: Specify the number of seconds that the appliance waits for a response from the RADIUS server.
Retries: Specify how many times the appliance attempts to contact an authentication RADIUS server.

The default is 5.

If you have configured multiple RADIUS servers for authentication and the NIOS appliance fails to contact the first server in the list, it tries to contact the next server, and so on.

Accounting: Optionally, modify the Accounting settings.

- Retries: Specify how many times the appliance attempts to contact an accounting RADIUS server. The default is 1000.
- Mode: Specifies how the appliance contacts the RADIUS servers. The default is Ordered List.
  - Ordered List: The Grid member always selects the first RADIUS server in the list when it sends an authentication request. It queries the next server only when the first server is considered down.
  - Round Robin: The Grid member sends the first authentication request to a server chosen randomly in a group. If there is no response from the server, the Grid member selects the next server in the group. Continued attempts are performed sequentially until it selects the last server in the group. Then it starts with the first server in the group and continues the selection process until all the servers have been attempted.
- Comment: Enter useful information about the RADIUS service.
- Disable: Select this to disable RADIUS authentication for the servers listed in the table.

4. Save the configuration and click Restart if it appears at the top of the screen.

Note that the following fields in the wizard do not apply to this feature: Enable NAC Filter, Cache Time to Live, and Recovery Interval. They are used with the NAC Integration feature described in Chapter 32, Authenticated DHCP.

Authenticating Admins Using Active Directory

Active Directory™ (AD) is a distributed directory service that is a repository for user information. The NIOS appliance can authenticate admin accounts by verifying user names and passwords against Active Directory. In addition, the NIOS appliance queries the AD domain controller for the group membership information of the admin. The appliance matches the group names from the domain controller with the admin groups on its local database. It then authorizes services and grants the admin privileges, based upon the matching admin group on the appliance.

Figure 4.6 Authentication Using a Domain Controller

To configure NIOS to authenticate administrators using Active Directory domain controller groups, you must first configure user accounts on the domain controller. Then, on the NIOS appliance, do the following:

- Configure one or more AD authentication server group on the appliance and add AD domain controllers to the group. For information about configuring an AD authentication service group for admins, see bookmark460.
- If you configured admin groups on the AD controller, you must create those same groups on the NIOS appliance and specify their privileges and settings. Note that the admin group names must match those on the AD domain controller. You can specify a default group as well. The NIOS appliance assigns admins to the default group if none of the admin groups on the NIOS appliance match the admin groups on the AD domain controller or if there are no other admin groups configured. For information about configuring group permissions and privileges, see About Admin Groups.
- Add the newly configured Active Directory service to the list of authentication services in the admin policy, and add the admin group names as well. See Defining the Authentication Policy for more information about configuring an admin policy.

Configuring an Active Directory Authentication Service Group
You can add multiple domain controllers to an AD authentication server group for redundancy. The NIOS appliance tries to connect with the first domain controller on the list. If it is unable to connect, it tries the next domain controller on the list, and so on.

To configure an Active Directory authentication server group on the NIOS appliance:

1. From the **Administration** tab, click the **Authentication Server Groups** tab.
2. Click the **Active Directory Services** subtab and click the **Add** icon.
3. In the **Add Active Directory Authentication Service** wizard, complete the following:
   - **Name**: Enter a name for the service.
   - **Active Directory Domain**: Enter the AD domain name.
   - **Domain Controllers**: Click the Add icon and complete the following to add an AD domain controller:
     - **Server Name or IP Address**: Enter the FQDN or the IP address of the AD server that is used for authentication.
     - **Comment**: Enter additional information about the AD server.
     - **Authentication Port**: Enter the port number on the domain controller to which the appliance sends authentication requests. The default is 389.
     - **Encryption**: Select SSL from the drop-down list to transmit through an SSL (Secure Sockets Layer) tunnel. When you select SSL, the appliance automatically updates the authentication port to 636. Infoblox strongly recommends that you select this option to ensure the security of all communications between the NIOS appliance and the AD server. If you select this option, you must upload a CA certificate from the AD server. Click **CA Certificates** to upload the certificate. In the **CA Certificates** dialog box, click the **Add** icon, and then navigate to the certificate to upload it.
     - **Connect through Management Interface**: Select this so that the NIOS appliance uses the MGMT port for administrator authentication communications with just this AD server.
     - **Disable server**: Select this to disable an AD server if, for example, the connection to the server is down and you want to stop the NIOS appliance from trying to connect to this server.
     - **Click Test** to test the configuration. If the NIOS appliance connects to the domain controller using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the server, the appliance displays a message indicating an error in the configuration.
     - **Click Add** to add the domain controller to the group.

When you add multiple domain controllers, the appliance lists the servers in the order you added them. This list also determines the order in which the NIOS appliance attempts to contact a domain controller. You can move a server up or down the list by selecting it and clicking the up or down arrow.

You can also delete a domain controller by selecting it and clicking the **Delete** icon.

- **Timeout(s)**: The number of seconds that the NIOS appliance waits for a response from the specified authentication server. The default is 5.
- **Comment**: Enter additional information about the service.
- **Disable**: Select this to retain an inactive AD authentication service profile.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Enabling Active Directory Authentication for Nested Groups

Windows servers support nesting groups in which you can add a group of admin users as a member of another group. Nested groups consolidate admin accounts and help reduce the number of permissions required for individual users or groups. In NIOS, you can enable nested group query so the appliance can recursively look up and use AD authentication service to authenticate members or admin accounts that are part of a nested group. When an admin belongs to multiple paths of hierarchy, you can enable nested group query in order to apply AD authentication service hierarchically in a parent-child structure. This enables the NIOS appliance to apply AD authentication service to all the groups of which an admin is a member. For example, if User 1 is a member of nested Group C, and Group C is a member of Group B, and Group B is a member of Group A, then the authentication service is applicable to all the groups of which User 1 is a member. In this example, the appliance performs a recursive lookup in Group C, Group B, and Group A while authenticating User 1.

To enable AD authentication for nested groups on the NIOS appliance:

1. From the **Administration** tab, click the **Authentication Server Groups** tab.
2. Click the **Active Directory Services** subtab and click the **Add** icon.
3. In the **Add Active Directory Authentication Service** wizard, complete the following:
   - **Nested Group Query**: This check box is deselected by default, meaning the nested group query is disabled. When nested group query is disabled, AD authentication service is applied to only one group of which the AD admin is a member. When you select this check box, AD authentication service is applied to all the nested groups of which an AD admin is a member. This setting is applicable to all the AD servers configured for the Active Directory authentication service.
4. Save the configuration.

### Authenticating Admin Accounts Using TACACS+

You can configure NIOS to authenticate admins against TACACS+ (Terminal Access Controller Access-Control System Plus) servers. TACACS+ provides separate authentication, authorization, and accounting services. To ensure reliable delivery, it uses TCP as its transport protocol, and to ensure confidentiality, all protocol exchanges between the TACACS+ server and its clients are encrypted. For detailed information about TACACS+, refer to the Internet draft [http://tools.ietf.org/html/draft-grant-tacacs-02](http://tools.ietf.org/html/draft-grant-tacacs-02).

In addition, you can configure a custom service, infoblox, on the TACACS+ server, and then define a user group and specify the group name in the custom attribute infoblox-admin-group. Ensure that you apply the user group to the custom service infoblox. On NIOS, you define a group with the same name and add it to the authentication policy.

Then when the TACACS+ server responds to an authentication and authorization request and includes the infoblox-admin-group attribute, NIOS
can match the group name with the group in the authentication policy and automatically assign the admin to that group. Figure 4.7 illustrates the TACACS+ authentication and authorization process when PAP/CHAP authentication is used.

**Figure 4.7 TACACS+ Authentication**

When you enable TACACS+ accounting, NIOS sends the TACACS+ accounting server a TACACS+ accounting event with the same information that it sends to the Audit Log for any user command/event. NIOS sends an accounting start packet when a user first logs in successfully using TACACS+ authentication, and it sends an accounting STOP packet when a user logs out of the GUI or CLI or when a GUI or CLI session times out. If a product restarts or software failure occurs, NIOS drops any outstanding accounting packets. Note that audit log entries that are greater than 3,600 characters are truncated in accounting events sent to TACAS+ servers.

**Configuring TACACS+**

Complete the following tasks to enable NIOS and the TACACS+ servers to communicate. On each TACACS+ server that you are adding to the authentication server group:

- For Windows TACACS+ servers, add the NIOS appliance as an AAA client. This step is not required for LINUX TACACS+ servers.
- Determine which user group on the TACACS+ server is used to match the admin group in NIOS, and then configure the following settings for the user group:
  - Add “infoblox” as a custom service.
  - Define the custom attribute for the group, in the format: `infoblox-admin-group=group_name`. For example, `infoblox-admin-group=remoteadmins1`. The group name can have a maximum of 64 characters.

On the NIOS appliance:

- Create a TACACS+ authentication server group. You can create only one TACACS+ server group. For more information, see Configuring a TACACS+ Authentication Server Group.
- Create the local admin group in NIOS that matches the user group on the TACACS+ server. Note that the NIOS admin group name must match the group name specified in the TACACS+ server and in the custom attribute. For example, if the custom attribute is `infoblox-admin-group=remoteadmins1`, then the admin group name must be `remoteadmins1`. In addition, you can designate a default admin group for remote admins. For information about configuring group permissions and privileges, see About Admin Groups.
- In the authentication policy, add the newly configured TACACS+ server group and the TACACS+ admin group name. See Defining the Authentication Policy for more information about configuring an admin policy.

**Configuring a TACACS+ Authentication Server Group**
You can add multiple TACACS+ servers to the TACACS+ authentication server group. NIOS sends authentication requests to the TACACS+ servers in the order they are listed. NIOS sends authentication requests to the first server on the list. If that server is unreachable or generates an error, then NIOS sends the request to the next server in the list that has not been previously queried, and so on. NIOS logs an error message in syslog if all servers have been queried and they all generate errors or are unreachable.

To configure a TACACS+ authentication server group:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Click the TACACS+ Services subtab and click the Add icon.
3. In the Add TACACS+ Service wizard, complete the following:
   - **Name:** Enter a name for the server group.
   - **TACACS+ Servers:** Click the Add icon and complete the following:
     - **Server Name or IP address:** The name or IP address of the TACACS+ server.
     - **Comment:** You can enter additional information about the server.
     - **Port:** The TCP destination port for TACACS+ communication. This port is used for authentication, accounting and authorization packets. The default is port 49.
     - **Authentication Type:** Select ASCII, PAP or CHAP. The default is CHAP.
     - **Shared Secret:** The shared key that the NIOS appliance and the TACACS+ server use to encrypt and decrypt messages.
     - **Enable Accounting:** Select this to enable NIOS to send accounting information to the TACACS+ server.
     - **Connect through Management Interface:** Select this check box to enable the appliance to use the MGMT port to communicate with the TACACS+ server. Ensure that the MGMT port is configured. Otherwise, the appliance will use the LAN interface.
     - **Disable Server:** Select this to prevent queries from being sent to this server. You can retain the configuration, but disable the service.
     - **Test** to test the configuration. Click **Add** to add the TACACS+ server to the list.
     - **Authentication/Authorization:** Optionally, modify the authentication and authorization settings. These settings apply to all TACACS+ servers that you configure on the NIOS appliance.
       - **Timeout(s):** Specify the number of seconds or milliseconds that the appliance waits for a response from the TACACS+ server before it tries to contact it again. The amount of time before the server is retried. The default and minimum is 5000, and the maximum is 60000.
       - **Retries:** Specify how many times NIOS attempts to contact a TACACS+ server and fails before it tries to contact the next server on the list. The default is 0. The maximum is 5.
     - **Accounting:** Optionally, modify the Accounting settings.
       - **Timeout(s):** Specify the number of seconds or milliseconds that the appliance waits for a response from the TACACS+ server. The amount of time before the server is retried. The default and minimum is 1000, and the maximum is 30000.
       - **Retries:** Specify how many times the appliance attempts to contact an accounting TACACS+ server and fails before it tries to contact the next accounting server on the list. The default is 0. The maximum is 5.
     - **Comment:** Enter additional information about the service.
   - **Disable:** Select this to retain an inactive TACACS+ authentication service profile.
4. Save the configuration.

**Authenticating Admins Using LDAP**

LDAP (Lightweight Directory Access Protocol) is an internet protocol for accessing distributed directory services. The NIOS appliance can authenticate admin accounts by verifying user names and passwords against LDAP. The NIOS appliance queries the LDAP server for the group membership information of the admin. The appliance matches the group names from the LDAP server with the admin groups in its local database. It then authorizes services and grants the admin privileges, based upon the matching admin group on the appliance. Figure 4.8 illustrates the LDAP authentication process.

*Figure 4.8 Authenticating using an LDAP server*
When you configure the NIOS appliance to authenticate admins against an LDAP server group, you must specify the authentication protocol of each LDAP server, which can be either anonymous or authenticated. The NIOS appliance connects anonymously to the LDAP server when the authentication type is anonymous. With authenticated type, the NIOS appliance connects using the bind DN and bind password defined for that server.

You can configure one of the following modes to send the authentication request to the LDAP server:

- **Ordered**: In this mode, the authentication request is sent to the first server in the list. The authentication request is sent to the next server only when the first server is out of service or unavailable.
- **Round Robin**: In this mode, the first authentication request is sent to a server chosen randomly in a group. If there is no response from the server, continued attempts are performed sequentially until it selects the last server in the list. Then it starts with the first server in the list and continues the selection process until all the servers have been attempted.

You can also specify the authentication type, for admins who belong to specific groups. The NIOS appliance uses the selected group authentication type to query the LDAP server and retrieve the group names to which the admin belongs. In LDAP, you can group users by any custom object classes. Example: objectclass groupofNames, objectclass posixGroup, etc. In NIOS, when you select Member Group Attribute as the group authentication type, the appliance uses custom LDAP group attributes to query the LDAP server and retrieve the group names for authentication. Example: memberOf, isMemberOf, etc. When you select Posix Group as the authentication type, the appliance uses "memberuid" and "objectClass" to query the server and retrieve the group names for authentication.

### Configuring LDAP

Do the following to configure NIOS to use one or more LDAP server groups to authenticate administrators:

- Configure at least one LDAP authentication server group. For more information, see Configuring an LDAP Server Group.
- Define admin groups for the admins that are authenticated by the LDAP servers and specify their privileges and settings. The group names in NIOS must match the admin group names on the LDAP server. For more information about defining admin groups, see About Admin Groups.
- In the authentication policy, add the LDAP server groups and the admin groups that match those on the LDAP server. You can also designate an admin group as the default group for remote admins. NIOS assigns admins to this group when it does not find a matching group for a remote admin. For more information about configuring the policy, see Defining the Authentication Policy.

### Configuring an LDAP Server Group

You can add one or more LDAP servers to an LDAP group for redundancy. The NIOS appliance tries to connect with the LDAP server based on the method you configure for the authentication request. If it does not receive a response within the configured timeout period and has tried to
connect the specified retry value, then it tries the next LDAP server on the list. The appliance makes a syslog entry when it fails to connect to any of the servers in the group and sends an SNMP trap and an email notification if configured. To configure an LDAP server group on the NIOS appliance:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Click the Add icon in the LDAP Services subtab.
3. In the Add LDAP Authentication Service wizard, complete the following:

   - **Name:** Enter the name of the server group.
   - **LDAP Servers:** Click the Add icon and enter the following:
     - **Server Name or IP Address:** Enter the FQDN (fully-qualified domain name) of the server or enter the IPv4/IPv6 address.
     - **LDAP Version:** Select the LDAP version. The NIOS appliance supports both LDAPv2 and LDAPv3. The default LDAP version is v3.
     - **Base DN:** Enter the base DN (Distinguished Name) value. All entries stored in an LDAP directory have a unique DN.
     - **Authentication Type:** Select the authentication type from the drop-down list. The supported authenticated types are as follows:
       - **Anonymous:** Select this to connect to the LDAP server anonymously. This is selected by default.
       - **Authenticated:** Select this to connect using the bind DN and bind password defined for that server.
     - **Bind User DN:** Enter the bind user DN.
     - **Bind Password:** Enter the bind password.
     - **Encryption:** Select the encryption type from the drop-down list.
       - **SSL:** This is selected by default. All the network traffic is encrypted through an SSL (Secure Sockets Layer) protocol. The appliance automatically updates the authentication port to 636 for SSL. You must upload a CA certificate that verifies the LDAP server certificate. Click **CA Certificates** to upload the certificate. In the **CA Certificates** dialog box, click the Add icon, and then navigate to the certificate to upload it.
       - **NONE:** Select this to unencrypt the connection. Note that Infoblox strongly recommends that you select the SSL option to ensure the security of all communications between the server and the member.
     - **Network Port:** Enter the authentication port number on the LDAP server to which the appliance sends authentication requests. The default value is 636. When you select NONE from the Encryption drop-down list, the appliance automatically updates the authentication port to 389.
     - **Comment:** Enter useful information about the LDAP server.
   - **Connect through Management Interface:** Select this so that the NIOS appliance uses the MGMT port for administrator authentication communications with just this LDAP server.
   - **Disable Server:** Select this to disable the LDAP server if, for example, the connection to the server is down and you want to stop the NIOS appliance from trying to connect to this server. You cannot disable the only server in a group if it is already being used by the remote authentication policy.
   - **Click Test** to test the configuration. If the NIOS appliance connects to the LDAP server using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the server, the appliance displays a message indicating an error in the configuration.
   - **Click Add** to add the LDAP server to the group. When you add multiple LDAP servers, the appliance lists the servers in the order you added them. This list also determines the order in which the NIOS appliance attempts to contact an LDAP server. You can move a server up or down the list by selecting it and clicking the up or down arrow.
   - **You can also delete a server by selecting it and clicking the Delete icon.**
     - **Server Timeout(s):** Specify the number of seconds that the appliance waits for a response from the LDAP server. The default value is 5 seconds.
     - **Retries:** Specify how many times the appliance attempts to contact an authentication LDAP server. The default value is 5.
       - If you have configured multiple LDAP servers for authentication and the NIOS appliance fails to contact the first server in the list, it tries to contact the next server after completing the specified number of attempts, and so on.
     - **Mode:** Select the order in which a Grid member connects to an LDAP server.
       - **Ordered List:** The Grid member always selects the first LDAP server in the list when it sends an authentication request. It queries the next server only when the first server is considered down. This is the default.
       - **Round Robin:** The Grid member selects the first authentication request to a server chosen randomly in a group. If there is no response from the server, the Grid member selects the next server in the group. Continued attempts are performed sequentially until it selects the last server in the group. Then it starts with the first server in the group and continues the selection process until all the servers have been attempted.
   - **Recovery Interval:** Specify the number of seconds that the appliance waits to recover from the last failed attempt in connecting to an LDAP server. Select the time unit from the drop-down list. The default is 30 seconds. This is the time interval that NIOS waits before it tries to contact the server again since the last attempt when the appliance could not connect to the LDAP server or when the LDAP server did not send a reply within the configured response timeouts and retry attempts.
   - **Group Authentication Type:** Select the group authentication type for LDAP authentication service from the drop-down list. By default, **Member Group Attribute** authentication type is selected. When you select **Member Group Attribute**, you can specify custom LDAP group attribute in the **Group Membership Attribute** field. For example, **memberOf, isMemberOf**, etc. The appliance uses this attribute to retrieve the group names to which the admin belongs. When you select **Posix Group**, the appliance uses "memberuid" and "objectClass" to retrieve the group names to which the admin belongs.
   - **Group Membership Attribute:** Specify the LDAP group attribute (such as "memberOf" and "isMemberOf"). This is used to query the server and retrieve the group names to which the admin belongs. This field is enabled only when you select **Member Group Attribute** in the **Group Authentication Type** drop-down list. The default value is **memberOf**.
   - **LDAP Search Scope:** To search for an admin user name in the LDAP directory, select one of the following LDAP search scope:
     - **Base:** Specify Base to perform search only on base in the LDAP directory. This is the top level of the LDAP directory tree.
     - **One Level:** Specify One Level to perform search on base DN and one level below the base in the LDAP directory.
     - **Subtree:** Specify Subtree to perform search on base and all the entries below the base DN in the LDAP directory. The default value is **One Level**.
• **User ID:** Specify the attribute associated with the user object in the LDAP server, such as "uid" and "cn". This attribute is used to match the NIOS user name.

• **Map LDAP Field to Extensible Attribute (for Captive Portal Users only):** If you configure the LDAP authentication server group to authenticate the captive portal users, you can map an LDAP attribute value to an existing extensible attribute. This mapping is optional. By doing so, the LDAP attribute value will be queried from the LDAP server once the captive portal user authentication is successful. The attribute value received from the LDAP server is mapped to the corresponding extensible attribute. NIOS updates or creates a MAC address filter depending on the captive portal user or the client's hardware and name.

Click the Add icon and enter the following:
- **LDAP Field:** Enter the LDAP attribute. This attribute is queried in the LDAP directory server.
- **Extensible Attributes:** Select an attribute from the drop-down list. The drop-down list displays only the extensible attributes configured with attribute type as string. Infoblox recommends that you avoid confidential data while mapping extensible attribute to an LDAP attribute because this data is visible in the extensible attribute field of the corresponding MAC address filter.

**Note:** Mapping an extensible attribute to an LDAP attribute must be unique for a given LDAP server. Attribute not defined in the LDAP directory for a given user is considered as null and is mapped to the corresponding extensible attribute with a default value. The default value of extensible attribute is Not Found. This default value is not configurable and they do not cause the authentication to fail.

• **Comment:** Enter useful information about the LDAP server group,

• **Disable:** Select this to disable the LDAP authentication server group. Note that you cannot disable an LDAP group if it is already being used to authenticate one or more administrators and/or captive portal users.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

**Defining the Authentication Policy**

The authentication policy defines which authentication server groups the appliance uses to authenticate admins and lists the local admin groups that map to the remote admin groups. By default, the appliance provides the "Local Admin" service for authenticating users against the local database. You cannot modify or delete this default service.

**Configuring a List of Authentication Server Groups**

To enable NIOS to use multiple authentication server groups, define a prioritized list as follows:

1. From the **Administration** tab, select the **Administrators** tab -> **Authentication Policy** tab.
2. From the **Authenticate users against these services in this order** section, click the Add icon to add an authentication server group.
3. Select one of the following in the **Add Authentication Service** section:
   - **Active Directory:** Select this to add an AD authentication server group, and then select a group from the drop-down list.
   - **RADIUS:** Select this to add a RADIUS authentication server group, and then select a group from the drop-down list.
   - **TACACS+:** Select this to add the TACACS+ authentication server group, and then select a group from the drop-down list.
   - **LDAP:** Select this to add the LDAP authentication server group, and then select a group from the drop-down list.
   - **Certificate Authentication Service:** Select this to add a certificate authentication service, and then select a service from the drop-down list.
4. Click **Add**.
   
   You can reorder the list by selecting an authentication server group and moving it up or down the list using the arrow keys.

**Configuring a List of Remote Admin Groups**

In order for NIOS to assign a remote admin to the correct group, you must list the admin groups in the local database that match the remote admin groups. You can also define a default admin group to which NIOS assigns remote users with no admin groups listed.

The appliance matches a remote admin to a group in the order the groups are listed. When the appliance receives information that an admin belongs to one or more groups, the appliance assigns the user to the first group in the list that matches. It assigns the admin to the default group, if specified, if no groups are returned by the authentication server, or if the appliance does not find a group in the local database that matches the group returned by the authentication server.

To configure the remote admin group list:

1. From the **Administration** tab, select the **Administrators** tab -> **Authentication Policy** tab.
2. In the **Authentication Server Groups is the authority for** section, select one of the following:
   - **Remote users, their passwords and their groups ownership:** Select this to use the authentication server groups to define the list of remote users, their passwords and their group ownerships. This is selected by default. You can add the list of admin groups to map the remote admin group to a local group in the **Map the remote admin group to the local group in this order** section.
   - **Passwords of Local users:** Select this to authenticate a remote user when you do not know to which remote admin group the user belongs.
   - **Map the remote admin group to the local group in this order:** In order for the appliance to assign a remote admin to the correct group, you must list the admin groups in the local database that match the remote admin groups. The appliance matches a remote admin to a group in the order the groups are listed. You can also define a default admin group to which NIOS assigns remote users with no admin groups listed. This section is disabled when you select **Passwords of Local users** in the **Authentication Server Groups is the authority for** section.
When the appliance receives information that the admin belongs to one or more groups, the appliance selects the first group in the list that matches, and assigns that group to the admin. If no groups are returned by the authentication server, the default group is assigned (if specified).

Complete the following to configure the remote admin group list:

- Click the Add icon to add an admin group to the list. In the Admin Group Selector dialog box, select an admin group.
- Use Shift+click and Ctrl+click to select multiple admin groups.
- You can reorder the list by selecting an admin group and using the arrow keys to move it up or down the list.
- **Assign user to this group if remote admin group cannot be found:** Click Select to assign a user to a specific admin group if the remote admin group is not found. In the Admin Group Selector dialog box, select an admin group. You can also click Clear Selection to clear the displayed member and select a new one.

### Authenticating Admins Using Two-Factor Authentication

You can configure NIOS to use the two-factor authentication method to authenticate users based on X.509 client certificates. In two-factor authentication, NIOS first negotiates SSL/TLS client authentication to validate client certificates. It then authenticates the admins based on the configured authentication policy. You must first configure an authentication policy, and then configure and enable the certificate authentication service for the two-factor authentication to take effect. NIOS uses certificate authentication service as the authentication policy. For information about how to set up an authentication policy, see [Defining the Authentication Policy](#).

Using the certificate authentication service, you can choose how the client certificate associates with the CA certificate. NIOS allows you to associate the client certificate manually and automatically. With manual certificate binding option, you must associate a certificate for a particular user manually, which is verified with the CA certificate. With automatic match policy, NIOS extracts the username from the client certificate, which is then matched with the certificate authentication service. When you configure certificate authentication service, NIOS searches the CA certificates associated with each admin group to detect a valid certificate authentication service for the client's certificate. You can either select a direct match or an automatic match for a certificate authentication service.

The Infoblox certificate authentication service uses the OCSP, which is an internet protocol that validates certificate status for X.509 digital certificates that are assigned to specific admins. NIOS allows you to choose Authority Information Access (AIA) extension from a certificate as a source of OCSP configuration or define OCSP servers manually. You can also disable OCSP check for a particular certificate authentication service. For more information about OCSP, refer to RFC 2560 at [http://tools.ietf.org/html/rfc2560](http://tools.ietf.org/html/rfc2560).

The status of these client certificates is stored on OCSP responders to which NIOS sends requests about certificate status. A certificate status can be "good," "revoked," or "unknown." After a successful SSL/TLS client authentication, NIOS authenticates the admin based on the configured authentication policy. If the authentication fails at this point, the appliance denies access to the admin. If the authentication policy has passed, the appliance sends a request to the OCSP responder for client certificate status about the admin. If the appliance receives a "good" status from the OCSP responder, the two-factor authentication is successful. The admin can now access the appliance. If the appliance receives a "revoked" or "unknown" status from the OCSP responder, the two-factor authentication fails. The admin cannot access the appliance even though the admin authentication policy has passed.

When there are multiple OCSP responders configured, the appliance contacts the responders based on their configured order. For the same client certificate, the appliance always takes the status reported by the first responder on the list that actually responds, even when there are different OCSP replies from different responders. When the appliance cannot contact the first responder or if the first responder does not reply, the appliance then takes the OCSP reply from the second responder and so on.

**Note:** Authentication for both the admin authentication policy and OCSP validation must be successful on NIOS.

*Figure 4.7 illustrates the two-factor authentication and authorization process.*
Best Practices for Configuring Two-Factor Authentication

Only superusers and limited-access users with the correct permissions can configure two-factor authentication. For information about admin roles and permissions, see Managing Admin Groups and Admin Roles. To configure two-factor authentication, consider the following:

- You must first set up an certificate authentication service and enable it.
- You can configure only one certificate authentication service that contains one or multiple OCSP responders to which NIOS sends requests about client certificate status. The appliance supports IPv4 and IPv6 OCSP responders.
- When you configure multiple OCSP responders, you can put them in an ordered list. The appliance contacts the first responder on the list. If the connection fails, it moves on to the second one, and so on. The result of the status check for a client certificate is based on the status reported by the first responder that replies.
- You can configure the timeout value and retry attempts that the appliance waits and tries before it moves on to the next OCSP responder.
- You can upload server certificates for each responder for OCSP response validation. You must upload an OCSP server certificate if you select the direct trust model.
- You can disable a specific responder if the server is out of service for a short period of time.
- Before you add an OCSP responder to the server group, you can test the server credentials.

To configure and enable two-factor authentication, complete the following tasks:

1. For local and remote authentication, ensure that the admin names for smart card users match the CNs (Common Names) used in the client certificates. For information about local and remote authentication, see About Admin Accounts.
2. Upload the CA (Certificate Authority) certificate, as described in About CA Certificates. The CA-signed certificates are used to validate OCSP server certificates and admin OCSP client certificates. Ensure that the CA certificate is in .PEM format. The .PEM file can contain more than one certificate.

Note: The uploaded CA certificates must be the ones that issued the client certificates to be authenticated. Otherwise, clients such as browsers, cannot establish a successful SSL/TLS client authenticated HTTPS session to the appliance.

3. Configure a certificate authentication service and enable it, as described in Configuring Certificate Authentication Services.
4. View certificate authentication services, as described in Viewing Certificate Authentication Services.
5. Modify certificate authentication services, as described in Modifying Certificate Authentication Services.
6. Delete certificate authentication services, as described in Deleting Certificate Authentication Services.

Note that once you save the certificate authentication service configuration, the appliance terminates administrative sessions for all admin users. After you enable the certificate authentication service, you can verify whether two-factor authentication is enabled. Go to the Administration -> Administrators -> Authentication Policy tab, Grid Manager displays the “Two-Factor Authentication Enabled” banner in this tab.

Configuring Certificate Authentication Services

To configure and enable the certificate authentication service, complete the following:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Click the Certificate Authentication Services subtab and click the Add icon.
3. In the Add Certificate Authentication Service wizard, complete the following:
   • Name: Enter a name for the certificate authentication service.
   • Username/password request: Select the check box if the certificate authentication service must request username and password from the user. When you select this check box, NIOS populates the username from the certificate and requests password from the user. If you do not select the check box, only the certificate is necessary to log in to the appliance. The appliance ignores the username and password when the user provides both. You can only see the login button and do not have to provide the password. The appliance displays the username when you click the login button.
   • Auto-populate username: Select a value from the drop-down list. You can define how the appliance must authenticate a particular user and its associated group. The values in the list are Auto-match and Direct-match. When you select Direct-match, NIOS searches for users with directly assigned certificates, which contains issuer details and serial attributes, in the local database. Users with directly assigned certificates can use certificate based authentication only.
   • Auto match by: Select a value from the drop-down list. This field is enabled only when you select Auto-match for Auto-populate username. NIOS extracts the username from the certificate and searches for it in effective authorization policies based on the configured match policies. The values in the list are:
     • AD Issuer Subject: Select this from the drop-down list to authenticate the user based on the Active Directory mentioned by the user.
     • SAN Email: Select this from the drop-down list to authenticate the user based on the email address in the SAN (Subject Alternative Name).
     • SAN UPN: Select this from the drop-down list to authenticate the user based on the UPN (User Principal Name) in the SAN (Subject Alternative Name).
     • Serial Number: Select this from the drop-down list to authenticate the user based on the serial number.
     • Subject DN Common Name: Select this from the drop-down list to authenticate the user based on the subject DN (Distinguished Name) common name. A Subject DN can include information about the user who is being authenticated, including common name, name of the organization, country code, and so on.
     • Subject DN Email: Select this from the drop-down list to authenticate a user based on the subject DN email address.
   • Enable remote lookup for user membership: Select the check box to enable lookup on remote servers. NIOS performs lookup against local users by default. For a remote lookup, you must specify the username and password for the authentication service. You can perform a look up for a user membership only if the remote service admin that is configured for remote lookup has enough permissions to read other user's membership information. You must also select the remote service that must be used for lookup. Note that NIOS supports remote lookup for Active Directories only.

   • Authentication Service: Select an authentication service from the drop-down list.
   • Service Account Credentials: Enter a username and password for authenticating lookup on remote servers.
   • Comment: Optionally, enter additional information about the certificate authentication service.
   • Disable: Select this check box to disable the record. Clear the check box to enable it.

4. Click Next to save the configuration and add OCSP responders to the table.
5. You can add multiple OCSP responders for failover purposes.
   • OCSP Check Type: Select a value from the drop-down list to perform OCSP checks. The values in the drop-down list are:
     • AIA and Manual: Select this from the drop-down list to use AIA (Authority Information Access) extension of X.509 certificate, when it is present, to authenticate the user. Note that AIA points to the certificate authentication service that is used to verify the certificate. If AIA is not available, then the authentication fails. If the certificate does not contain AIA, then the appliance uses manual OCSP for authentication.
     • AIA only: Select this from the drop-down list to use AIA only to authenticate the user. AIA points to the certificate authentication service that is used to verify the certificate. By selecting this option you restrict NIOS to use AIA only. If the certificate does not contain AIA or it is not complete, then the authentication fails.
     • Disabled: Select this from the drop-down list if you do not want to perform an OCSP check.
     • Manual: Select this from the drop-down list to define OCSP settings and upload CA certificates manually. When you select this option, NIOS ignores AIA even though it is present.
   • OCSP Responders: Click the Add icon and complete the following in the Add OCSP Responder section:
     • Server Name or IP Address: Enter the FQDN or the IP address of the OCSP responder that is used for authentication. The appliance supports IPv4 and IPv6 OCSP responders.
**Comment**: Enter useful information about the OCSP responder.
**Port**: Enter the port number on the OCSP responder to which the appliance sends authentication requests. The default is 80.
**Server Certificate**: Click Select to upload a server certificate. In the Upload dialog box, click Select to navigate to the certificate, and then click Upload. The appliance validates the certificate when you save the configuration. A server certificate is required for the direct trust model.
**Disable Server**: Select this check box to disable the OCSP responder if, for example, the connection to the server is down and you want to stop the NIOS appliance from trying to connect to this server.

**Note**: You cannot save the OCSP configuration when you disable all OCSP responders, thus the certificate authentication service is disabled and two-factor authentication is no longer in effect. You cannot add OCSP responders when you select AIA only or Disabled from the drop-down list for OCSP Check Type.

You can also click Test to test the configuration. If the appliance connects to the responder using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the responder, the appliance displays a message indicating an error in the configuration.

- **Response Timeout(s)**: Enter the time the appliance waits for a response from the specified OCSP responder.
- **Retries**: Enter the number of times the appliance tries to connect to the responders after a failed attempt.
- **Recovery Interval**: Enter the time the appliance waits to recover from the last failed attempt in connecting to an OCSP responder. Select the time unit from the drop-down list. The default is 5.
- **Trust Model**: Select Direct or Delegated from the drop-down list as the trust model for OCSP responses. In a direct trust model, OCSP responses are signed with an explicitly trusted OCSP responder certificate. You must upload the OCSP responder certificate if you select Direct. In a delegated trust model, OCSP responses are signed with a trusted CA certificate. A server certificate is not required when you select Delegated. The default is Direct.

6. Click Next to save the configuration and associate CA Certificates with the respective certificate authentication service. You can associate multiple CA certificates with the service.

Note that enabling the certificate authentication service terminates administrative services for all users. Ensure that you have uploaded the correct CA certificates before enabling the service. Your login names must also match the common name used in the certificate. When you configure multiple OCSP responders, ensure that you place them in the correct order because the status check for a client certificate is based on the OCSP reply sent by the first OCSP responder that replies.

NIOS detects a valid certificate authentication service for a client's certificate by searching through the assigned CA certificates for each group. NIOS matches issuer field in the client's certificate with the CA certificate to find the appropriate match. Note that the subject in CA certificate must match the issuer in the client's certificate and corresponding certificate authentication service. You cannot assign several CA certificates with the same issuer to the same certificate authentication service.

Note the following about the certificate authentication service:

- You cannot assign various CA certificates with the same issuer to the same certificate authentication service.
- You cannot assign the same CA certificate to the same group twice or to a different certificate authentication service. However, different certificate authentication services can contain CA certificates with the same subject. To distinguish such groups you can use **Client Subject name** to determine which certificate must match the CA certificate to be associated with the certificate authentication service. If the client certificate does not match any certificate authentication service, then the authentication fails. A CA certificate verifies the client certificate.

7. Click Add to associate CA certificates with the certificate authentication service. The following information is displayed when you associate a CA certificate:

- **Subject**: The name of the certificate.
- **Issuer**: The name of the trusted CA that issued the certificate.
- **Valid From**: The date from which the certificate becomes valid.
- **Valid To**: The date until which the certificate is valid. You can do the following:
  - Select a certificate and click the Delete icon to delete it.
  - Print the data or export it in .csv format.

You can also do the following for a certificate authentication service:
Use **Global Search** to search for certificate authentication services. For information, see **Global Search**.

View audit log entries for the certificate authentication service. For information, see **Viewing the Audit Log**.

Select a certificate authentication service and click the Delete icon to delete it. In the **Delete Confirmation** dialog box, click **Yes** to confirm deletion.

Modify a certificate authentication service as mentioned in **Modifying Certificate Authentication Services**.

Print the data or export it in .csv format.

---

**Enabling Certificate Authentication Service for a User**

You can restrict users to use certificate based authentication only. Note that certificate authentication service with a direct-match searches only for users with certificate authentication service enabled. Such users are successfully authenticated by the certificate authentication service using auto-match.

1. From the **Administration** tab, click the **Administrators** tab -> **Admins** tab -> **admin_account** check box, and then click the **Edit** icon.
2. In the **Administrator** editor, click the **General** tab, and then click the **Advanced** tab.
3. In the **General Advanced** tab, complete the following:
   - **Enable Certificate Authentication**: Select this check box to enable certificate authentication for the selected user. You must configure certificate authentication service and associate a valid client CA certificate with the selected user. This is disabled by default.
   - **Client Certificate Number**: You can specify a client certificate number only when you select the **Enable Certificate Authentication** check box. This is disabled by default. Enter the serial number as mentioned in the certificate. Examples: 397F9435000100000032 (hexadecimal format), 123 (decimal format), and so on.
   - **Client CA Certificate**: You must associate a CA certificate that signs the client certificate. Click **Select** to associate a CA certificate.
     When you select a CA certificate from the list, NIOS displays the subject of the selected CA certificate. The **CA Certificate Selector** dialog box displays the following information about CA certificates:
       - **Issuer**: The name of the trusted CA that issued the certificate.
       - **Valid From**: The date from which the certificate becomes valid.
       - **Valid To**: The date until which the certificate is valid.
       - **Subject**: The name of the certificate.
     Click **OK** to select and associate the client CA certificate with the selected admin user.
4. Save the configuration.

**Viewing Certificate Authentication Services**

To view the certificate authentication service, complete the following:

1. From the **Administration** tab, click the **Authentication Server Groups** tab.
2. Click the **Certificate Authentication Services** subtab.
3. Grid Manager displays the following about the certificate authentication service:
   - **Name**: The name of the certificate authentication service.
   - **Comment**: Comments about the certificate authentication service.

You can also display the following column:
- **Disabled**: Indicates if the certificate authentication service is enabled or disabled.

You can do the following in this tab:
- Sort the data in ascending or descending order by column.
- Select the certificate authentication service and click the **Edit** icon to modify data, or click the **Delete** icon to delete it.
- Print and export the data in this tab.

**Modifying Certificate Authentication Services**

To modify a certificate authentication service:

1. From the **Administration** tab, click the **Authentication Server Groups** tab -> **Certificate Authentication Services** subtab -> select a certificate authentication service, and then click the **Edit** icon.
2. The **Certificate Authentication Service** editor provides the following tabs from which you can modify data:
   - **General**: In this tab, modify certificate authentication service data, as described in **Configuring Certificate Authentication Services**.
   - **OCSP**: Modify associated OCSP responders. For more information, see **Configuring Certificate Authentication Services**.
   - **CA**: Add and delete CA certificates that are associated with the certificate authentication service. For more information, see **Configuring Certificate Authentication Services**.
3. Save the configuration.

**Deleting Certificate Authentication Services**
You can delete a certificate authentication service any time after you have created it. To delete a certificate authentication service:

1. From the Administration tab, click the Authentication Server Groups tab -> Certificate Authentication Services subtab, select a certificate authentication service and then click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes.

Changing Password Length Requirements

Password length requirements control how long a password must be for a NIOS appliance admin account. Increasing this value reduces the likelihood of hackers gaining unauthorized access.

To change password length requirements:

1. From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the Password tab.
3. Enter a number from 4 to 64 in the Minimum Password Length field.
4. Save the configuration and click Restart if it appears at the top of the screen.

Notifying Administrators

You can notify individual administrators about system status through email, or notify a group of people using an alias email address. If you have configured DNS resolution on your network, the E-mail relay configuration function is not required. If you did not configure the settings on the DNS Resolver section, you must enter a static IP address of the target system in the Relay Name/IP Address field. The appliance sends e-mail to administrators when certain events occur. This functionality supports both IPv4 and IPv6 networks. Here is a list of events that trigger e-mail notifications:

- Changes to link status on ports and online/offline replication status
- Events that generate traps, except for upgrade failures (ibUpgradeFailure). For a list of events, see Infoblox MIBs

The appliance attempts to send the email notification once after an event. It does not try to send the notification again, if the first attempt fails. Infoblox recommends that you use the Test Email settings button to test the email settings and to verify that the recipient received the notification.

You can define the email settings at the Grid and member levels.

Grid Level

To notify an administrator of an independent appliance or a Grid:

1. From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the Email tab, and then complete the following:
   - Enable Email notification: Select this.
   - Email address: Enter the email address of the administrator. Use an email alias to notify multiple people.
   - Use SMTP Relay: Select this if the NIOS appliance must send email to an intermediary SMTP (Simple Mail Transfer Protocol) server that relays it to the SMTP server responsible for the domain name specified in the email address. Some SMTP servers only accept email from certain other SMTP servers and might not allow email from the NIOS appliance. In this case, specify the DNS name or IP address of a different SMTP server that does accept email from the NIOS appliance and that will then relay it to the SMTP server that can deliver it to its destination. Clear this if it is unnecessary to use an email relay server.
   - SMTP Relay Name or Address: If you have configured DNS resolution, enter the DNS name of the relay server. If DNS resolution is not configured, enter the IP address of the relay server.
3. Optionally, click Test Email settings to confirm this feature is operating properly.
4. Save the configuration and click Restart if it appears at the top of the screen.

Member Level

To define email settings for a member:

1. From the Grid tab, select the Grid Manager tab -> member check box, and then select the Edit icon.
2. In the Grid Member Properties editor, select the Email tab, and then click Override to override Grid-level settings.
3. Complete the email configuration as described in Grid Level.

Administrative Permissions for Common Tasks

Table 4.7 lists some of the common tasks admins can perform and their required permissions. Table 4.12 lists tasks related to device discovery, with their required permissions.

All the permission tables in this chapter use the following definitions:

- **RW** = Read/Write permission
- **RO** = Read-only permission

Table 4.7 Permissions for Common Tasks
### Administrative Permission for the Grid

By default, the Grid Master denies access to Grid members when a limited-access admin group does not have defined permissions. You can grant an admin group read-only or read/write permission, or deny access to all Grid members or you can grant permission to specific Grid members, as described in Applying Permissions and Managing Overlaps.

Note: Only superusers can modify DNS and DHCP Grid properties.

The following sections describe the types of permissions that you can set with Grid permissions:

- **Administrative Permissions for Grid Members**
- 4823698
- 4823698
- 4823698

### Administrative Permissions for Grid Members

4823698 lists the tasks admins can perform and the required permissions for Grid members.

**Table 4.8 Grid Member Permissions**
<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member (s)</th>
<th>Member DNS Properties</th>
<th>Member DHCP Properties</th>
<th>Restart Member DNS</th>
<th>Restart Member DHCP</th>
<th>DNS Views</th>
<th>DNS Zones</th>
<th>Networks</th>
<th>DHCP Range s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign member to DNS zones</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
</tr>
<tr>
<td>Assign member to networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
</tr>
<tr>
<td>Assign member to DHCP ranges</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
</tr>
<tr>
<td>Configure member properties</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add a member to a Match Members list of a DNS view</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
</tr>
<tr>
<td>Delete a view with members in a Match Members list</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RO</td>
</tr>
<tr>
<td>View DNS and DHCP member properties</td>
<td></td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and download syslog</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View DNS and DHCP configuration file</td>
<td></td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View network statistics</td>
<td></td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart DNS service on the member</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
</tr>
<tr>
<td>Restart DHCP service on the member</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
</tr>
</tbody>
</table>

**Administrative Permissions for Network Discovery**
Limited-access admin groups can initiate a discovery and manage discovered data based on their administrative permissions. You can set global permissions for network discovery as described in [Defining Global Permissions](#). The following table lists the tasks admins can perform and the required permissions for network discovery.

*Table 4.9 Permissions for Network Discovery*

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Network Discovery</th>
<th>DNS Zones</th>
<th>Networks Selected for Discovery</th>
<th>Port Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate and control a discovery on selected networks</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View discovered data</td>
<td></td>
<td></td>
<td></td>
<td>RO</td>
</tr>
<tr>
<td>Add unmanaged data to existing hosts, and resolve conflicting IP addresses</td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
</tr>
<tr>
<td>Convert unmanaged data to a host, fixed address, reservation, A record, or PTR record</td>
<td></td>
<td></td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Configure device interfaces, provision networks on interfaces, de-provision networks</td>
<td></td>
<td></td>
<td>RW</td>
<td>RW</td>
</tr>
</tbody>
</table>

**Administrative Permissions for Scheduling Tasks**
You can schedule tasks, such as adding hosts or modifying fixed addresses, for a future date and time. To schedule tasks, you must first enable the scheduling feature at the Grid level, and then define administrative permissions for admin groups and admin roles. For information, see [Scheduling Tasks](#). Only superusers can enable and disable this feature and grant scheduling permissions to admin groups. Limited-access admin
groups can schedule tasks only when they have scheduling permissions.
Superusers can do the following:

- Enable and disable task scheduling at the Grid level
- Grant and deny scheduling permissions to admin groups and admin roles
- Schedule tasks for all supported object types
- Reschedule and delete any scheduled task

You can set global permissions to schedule tasks as described in Defining Global Permissions. The following table lists the tasks admins can perform and the required permissions. Users with read/write permission to scheduling can view, reschedule, and delete their own scheduled tasks.

Table 4.10 Scheduling Task Permissions

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Scheduling Task</th>
<th>All Networks</th>
<th>All DNS Views</th>
<th>All Shared Record Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule the addition, modification, and deletion of all supported object types</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>View, reschedule, and delete scheduled tasks</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Convert unmanaged data to a host, fixed address, reservation, A record, or PTR record</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
</tr>
</tbody>
</table>

To schedule tasks for specific resources, admins must have Read/Write permission to scheduling tasks, plus the required permissions to the supported resources. For information about permissions for specific resources, see the following:

- Grid members—See Administrative Permission for the Grid.
- DNS resources—See 4823698.
- DHCP resources—See Administrative Permissions for DHCP Resources.

Note that the appliance deletes all pending scheduled tasks when superusers disable task scheduling at the Grid level. The appliance deletes an admin's scheduled tasks when superusers do the following:

- Set the scheduling permission of admin groups and roles to “Deny”
- Delete or disable an admin group or an admin role
- Delete or disable local admins
- Delete the scheduling permission from any admin group or admin role that contains users with pending scheduled tasks
- Change the admin group of a limited-access admin

Administrative Permissions for Microsoft Servers

By default, only superusers can add Microsoft servers as managed servers to the Grid. Limited-access admins can add and manage Microsoft servers from the Grid based on their administrative permissions.

The following table lists the tasks admins can perform and the required permissions. Note that only superusers can add a Microsoft server to a name server group.

Table 4.11 Microsoft Server Permissions

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Microsoft Server(s)</th>
<th>Grid Member(s)</th>
<th>Network Views</th>
<th>DNS Views</th>
<th>DNS Zones</th>
<th>Resource Records</th>
<th>Networks</th>
<th>DHCP Ranges</th>
<th>Superscopes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign Microsoft server to member</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a network view to the Microsoft server</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a DNS view to the Microsoft server</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign Microsoft server as primary or secondary to DNS zones</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity</td>
<td>Permissions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove a Microsoft server as the primary or secondary server of a zone</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove a zone from a Microsoft server</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit zones and resource records of Microsoft servers</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a Microsoft server to a network</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign a Microsoft server to a DHCP range</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove a network served by a Microsoft server</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove a DHCP range (scope) from a Microsoft server</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add, modify and remove Microsoft superscopes</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear leases from Microsoft server</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit Microsoft server properties</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Microsoft server properties</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and download Microsoft logs</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start/Stop DNS or DHCP on the Microsoft server</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove a Microsoft server from the Grid</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Administrative Permissions for IPAM Resources**

Limited-access admin groups can access certain IPAM resources only if their administrative permissions are defined. By default, the appliance denies access when a limited-access admin group does not have defined permissions. You can grant admin groups read-only or read/write permission, or deny access to the following IPAM resources:

- Network views
- IPv4 networks
- IPv6 networks
- Hosts

The appliance applies permissions for IPAM resources hierarchically. Permissions to a network view apply to all networks and resources in that view. You can also grant an admin group broad permissions to IPAM resources, such as read/write permission to all IPv4 networks and IPv6 networks in the database. In addition, you can grant permission to a specific host in a network. Permissions at more specific levels override global permissions.

The following sections describe the types of permissions that you can set for IPAM resources:

- **Administrative Permissions for Network Views**
- 4823698
- 4823698
Administrative Permissions for IPv4 and IPv6 Networks

Limited-access admin groups can access IPv4 and IPv6 networks only if their administrative permissions are defined. Permissions for a network apply to all its DNS and DHCP resources, if configured. To override network-level permissions, you must define permissions for specific objects within the networks. You can also define permissions for specific DHCP objects and Grid member to restrict admins to perform only the specified DHCP tasks on the specified member. For more information, see Defining DNS and DHCP Permissions on Grid Members.

You can grant read-only or read/write permission, or deny access to networks, as follows:

- All IPv4 or IPv6 networks—Global permission that applies to all networks in the database.
- A specific network—Network permissions apply to all objects in the network. This overrides global permissions.
- A specific network on a specific member—Network permissions apply to all objects in the network and member permissions apply to the specific member. For information about member permissions, see Modifying Permissions on a Grid Member.

Administrative Permissions for Hosts

A host record can contain both DNS and DHCP attributes if you configure them. When applying administrative permissions to host records, the permissions apply to all relevant DNS and DHCP resources within the host records. You can define global permissions to all hosts. To override global permissions, you must define permissions for specific hosts.

You can grant read-only or read/write permission, or deny access to host records, as follows:

- All hosts—Global permission that applies to all host records in the Grid.
- A specific host—Object permission that applies only to a selected host.

Administrative Permissions for DHCP Fingerprint Permissions

NIOS provides a global permission for all All DHCP Fingerprint; however, it does not support object level permissions for fingerprints. To use fingerprint filters, you must have superuser privileges.

Administrative Permissions for Network Insight Tasks

4823698 summarizes the permissions you need to perform various tasks related to device discovery.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Network Discovery</th>
<th>DNS Zones</th>
<th>Networks Selected for Discovery</th>
<th>Port Control</th>
<th>All Network Views / All IPv4 Networks / All IPv6 Networks</th>
<th>Permissions for Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate and control a discovery on selected networks</td>
<td>RW</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View discovered data</td>
<td></td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resolve conflicting IP addresses</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Convert unmanaged objects to a host, fixed address, reservation, A record, or PTR record</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure device interfaces, provision networks on interfaces</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure a Blackout schedule for networks or DHCP ranges</td>
<td>RW</td>
<td></td>
<td></td>
<td>RO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Creating/editing port reservations for a Grid member, host, fixed address, reservation, A record, or PTR record

**Administrative Permissions for DNS Resources**

You can grant roles and admin groups read-only or read/write permission, or deny access to the following DNS resources:

- DNS Views
- DNS Zones
- Response Policy Zones
- All RPZ Rules
- Hosts
- Bulk Hosts
- A records
- AAAA records
- CNAME records
- DNAME records
- MX records
- PTR records
- SRV records
- TXT records
- Hosts
- Bulk Hosts
- Shared Record Groups
- Shared A records
- Shared AAAA records
- Shared CNAME records
- Shared DNAME records
- Shared MX records
- Shared SRV records
- Shared TXT records
- DNS64 synthesis groups
- Adding a blank A/AAAA record

The appliance applies permissions for DNS resources hierarchically. Permissions to a DNS view apply to all zones and resource records in that view. Permissions for a zone apply to all its subzones and resource records, and resource record permissions apply to those resource records only. To override permissions set at higher level, you must define permissions at a more specific level. To assign permissions, see Applying Permissions and Managing Overlaps.

You can also define permissions for specific DNS objects and Grid member to restrict admins to perform only the specified DNS tasks on the specified member. For more information, see Defining DNS and DHCP Permissions on Grid Members.

The following sections describe the different types of permissions that you can set for DNS resources:

- 4823700
- 4823700
- 4823700

**Administrative Permissions for DNS Views**

Limited-access admin groups can access DNS views, including the default view, only if their administrative permissions are defined. Permissions to a DNS view apply to all its zones and resource records. To override view-level permissions, you must define permissions for its zones and resource records. For example, you can grant an admin group read-only permission to a view and read/write permission to all its zones. This allows the admins to display the view properties, but not edit them, and to create, edit and delete zones in the view.

You can grant read-only or read/write permission, or deny access to DNS views, as follows:

- All views—Global permission that applies to all DNS views in the database.
- A specific view—Applies to its properties and its zones, if you do not define zone-level permissions. This overrides the global view permissions.
- All zones in a view—If you do not define permissions for zones, they inherit the permissions of the view they are in.

For information on setting permissions for a view and its zones, see Applying Permissions and Managing Overlaps.

The following table lists the tasks admins can perform and the required permissions for DNS views.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member(s)</th>
<th>All DNS Views</th>
<th>Specific DNS View</th>
<th>All DNS Zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete DNS views</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete DNS zones with assigned members</td>
<td>RW</td>
<td></td>
<td></td>
<td>RW</td>
</tr>
<tr>
<td>Tasks</td>
<td>Grid Member(s)</td>
<td>Specific DNS View</td>
<td>All DNS Zones</td>
<td>Specific DNS Zone</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------</td>
<td>-------------------</td>
<td>---------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Create, modify, and delete DNS zones without assigned members</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete a specific DNS view</td>
<td>RW</td>
<td></td>
<td>ME</td>
<td></td>
</tr>
<tr>
<td>Add Grid members to a Match Members list of a DNS view</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete a DNS view with Grid members in a Match Members list</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View DNS view properties, DNS zones, and resource records</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View DNS zone properties, subzones, and resource records</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart services from the DNS tab</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Administrative Permissions for Zones**

By default, zones inherit administrative permissions from the DNS view in which they reside. You can override view-level permissions by setting permissions for specific zones. Permissions set for a zone are inherited by its subzones and resource records. To override zone-level permissions, set permissions for specific subzones and resource records.

For example, you can grant an admin group the following permissions:

- Read-only to a zone and to all its A, AAAA, and PTR records (in reverse and forward-mapping zones)
- Read/Write permission to all MX and SRV records in the zone
- Deny to all the other resource records—CNAME, DNAME, TXT, host, and bulk host
- You can grant read-only or read/write permission, or deny access to zones as follows:
  - All zones—Global permission that applies to all zones in all views.
  - All zones in a view—Permissions at this level override the global permissions.
  - A specific zone—Applies to the zone properties and resource records. If you do not define permissions for its resource records, this overrides global and view-level permissions. If you delete a zone and reparent its subzone, the subzone inherits the permissions of the new parent zone.
  - All Response Policy Zones—Global permission that applies to all the Response Policy Zones.
  - All Response Policy Rules—Global permission that applies to all the local Response Policy Zone rules.

**Note:** Object permissions are not applicable to Response Policy Zone rules.

Each resource record type in a zone—for example, you can define permissions for all A records and for all PTR records in a zone. If you do not define permissions for resource records, they inherit the permissions of the zone in which they reside.

For information on setting permissions for zones and resource records, see [Applying Permissions and Managing Overlaps](#).

The following table lists the tasks admins can perform and the required permissions for zones.

**Table 4.14 DNS Zone Permissions**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member(s)</th>
<th>Specific DNS View</th>
<th>All DNS Zones</th>
<th>Specific DNS Zone</th>
<th>Resource Records</th>
<th>Shared Record Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete zones, subzones and resource records with assigned members</td>
<td>RW</td>
<td></td>
<td>ME</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete zones, subzones and resource records without assigned members</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lock and unlock a zone</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete a zone with assigned Grid members</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete all zones, subzones, and resource records in a specific view</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Assign a name server group (member) to a zone | RW | RW |
Delete a zone with name server groups assigned | RW | RW |
Assign a shared record group to a zone | RW | RW |
View zone properties, subzones, and resource records of a specific zone | RO |
Search for zones, subzones, and resource records in a specific DNS view | RO | RO |
Copy resource records from one zone to another: Source zone | RO | RO |
Copy resource records from one zone to another: Destination Zone | RW | RW |

**Administrative Permissions for Resource Records**

Resource records inherit the permissions of the zone to which they belong. You can override zone-level permissions by setting permissions for specific resource records.

You can grant read-only or read/write permission, or deny access to resource records as follows:

- Each resource record type in all zones and in all views—Global permission that applies to all resource records of the specified type; for example, all A records in the database.
- Each resource record type in a zone—Permissions at this level override global permissions.
- A specific resource record—Overrides zone-level permissions.

For information on setting permissions for resource records, see *Applying Permissions and Managing Overlaps*. The following table lists the tasks admins can perform and the required permissions for resource records.

<table>
<thead>
<tr>
<th>Table 4.15 DNS Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasks</td>
</tr>
<tr>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Create, modify, and delete resource records for a specified type, such as all A records or all PTR records</td>
</tr>
<tr>
<td>View resource records for a specified type only</td>
</tr>
<tr>
<td>Search for records of a specified type</td>
</tr>
<tr>
<td>View a specific resource record</td>
</tr>
<tr>
<td>View, modify, and delete a specific resource record</td>
</tr>
</tbody>
</table>

The following are additional guidelines:

- Only admins with read/write permission to bulk host records and read/write permission to reverse zones can create bulk host records and automatically add reverse-mapping zones.
- To create host records, admins must have read/write permission to the network and zone of the host.
- Admins must have read-only permission to the host records in a zone to view the Host Name Compliance Report. Admins must have read/write permission to the resource records in a zone to modify host names that do not comply with the host policy.
Administrative Permissions for Adding Blank A or AAAA Records

By default, only superusers can add and edit A, AAAA, shared A, and shared AAAA records with a blank name. Limited-access admin groups can add and edit A, AAAA, shared A, and shared AAAA records with a blank name, only if their administrative permissions are defined. You can grant read/write or deny permission to Adding a blank A/AAAA record for specific admin groups, which applies to all admin roles in the group. You can define global permissions for specific admin groups and roles to allow limited-access users to add and edit blank A, AAAA, shared A, and shared AAAA records, as described in Defining Global Permissions.

Administrative Permissions for Shared Record Groups

By default, only superusers can add, edit, and delete shared record groups. Limited-access admin groups can access shared record groups, only if their administrative permissions are defined. You can set different permissions for a shared record group and for each type of shared resource record in the group. For example, you can grant a role or an admin group the following permissions:

- Read-only to a shared record group and to all its shared A, AAAA, and CNAME records
- Read/Write permission to all the shared MX and SRV records in the shared record group
- Deny to the TXT records

You can grant read-only or read/write permission, or deny access to shared record groups, as follows:

- All shared record groups—Global permission that applies to all shared record groups in the database.
- A specific shared record group—Overrides global permissions.
- Each shared record type in all shared record groups — The shared resource record types include shared A records, shared AAAA records, shared CNAME records, shared MX records, shared SRV records, and shared TXT resource records.
- Each shared record type in a shared record group—Permissions at this level override global permissions.
- A specific shared record—Overrides zone-level permissions. Note the following guidelines:
  - Shared record group permissions override zone permissions.
  - Even if a zone is locked, superusers and limited-access users with read/write access can still edit or delete a shared record in the zone.

For information on setting permissions for shared record groups, see Applying Permissions and Managing Overlaps. The following table lists the tasks admins can perform and the required permissions for shared record groups.

**Table 4.16 Permissions for Shared Record Groups**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All Shared Record Groups</th>
<th>Specific Shared Record Group</th>
<th>Shared Record Type</th>
<th>Specific DNS Zone</th>
<th>Specific Shared Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete shared record groups</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete a shared record group</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View a shared record group</td>
<td></td>
<td></td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete shared records for a specific type</td>
<td></td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View or search for shared records of a specific type</td>
<td></td>
<td></td>
<td></td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete shared records for a specific type in a specified shared record group</td>
<td></td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View shared records for a specific type in a specified shared record group only</td>
<td></td>
<td></td>
<td>RO</td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete a shared record</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
</tr>
<tr>
<td>View a specific shared record</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RO</td>
</tr>
</tbody>
</table>
Assign a shared record group to DNS zones

Change the DNS zones associated with a shared record

Delete zones with a shared record group assigned. Before you delete a shared record group, you must remove all zones associated with it.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All Synthesis Groups</th>
<th>Specific Synthesis Group</th>
<th>Grid</th>
<th>Specific Member</th>
<th>Specific DNS View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete synthesis groups</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete a specific synthesis group</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View a synthesis group</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply a synthesis group to the Grid</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply a synthesis group to a member</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply a synthesis group to a DNS view</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Administrative Permissions for DNS64 Synthesis Groups**

By default, only superusers can add, edit, and delete DNS64 synthesis groups. Limited-access admin groups can access synthesis groups, only if their administrative permissions are defined.

You can grant read-only or read/write permission, or deny access to synthesis groups, as follows:

- All synthesis groups—Global permission that applies to all shared record groups in the database.
- A specific synthesis group—Overrides global permissions.

For information on setting permissions for synthesis groups, see Applying Permissions and Managing Overlaps. The following table lists the tasks admins can perform and the required permissions for synthesis groups.

**Table 4.17 Permissions for DNS64 Synthesis Groups**

**Administrative Permissions for DNS Resources with Associated IP addresses in Networks and Ranges**

You can further control permissions for DNS resources that have associated IP addresses in a network container, network, or address range. These DNS resources include A records, AAAA records, PTR records, and DNS hosts. Permissions for these resources have been added so you now have more control over who can perform which tasks for these DNS resources without affecting permissions defined for the networks and ranges to which the resources belong. For example, if you want to allow an admin to add, modify, and delete A records associated with IP addresses within a specific network but you do not want the same admin to modify or delete the network, you can grant the admin read-only permission for the specified network and read/write permission for A records in that network.

Similar behavior applies to AAAA records, PTR records, and DNS hosts.

As a superuser, you can now grant permissions to admin groups for more granular access to the following resources:

- IPv4 and IPv6 DHCP fixed addresses and IPv4 reservations in a range
- IPv4 and IPv6 host addresses in a range
- A and AAAA records in a network container, network, or range
- IPv4 and IPv6 PTR records in a network container, network, or range

For information about how to configure new permissions for these resources, see Configuring Permissions for DNS Resources in Networks and Ranges.
Best Practices for Configuring Permissions in Networks and Ranges

Before using permissions for DNS resources in networks and ranges, consider the following:

- You can enable and disable these permissions using the `set dns_perm_for_nw_range` CLI command. When you disable permissions after you have enabled and defined them, the appliance retains the permissions in an inactive mode. Inactive permissions are not verified nor displayed in Grid Manager. When you re-enable the permissions, the appliance activates them and displays them in Grid Manager. You can also use the `show dns_perm_for_nw_range` CLI command to verify the status of new permissions.

Note that permissions for fixed addresses and reservations are not controlled by the CLI command; they are always enabled. You can also enable and disable permissions for DNS Resources in Networks and Ranges through Grid Manager, as described in Enabling Permissions for DNS Resources in Networks and Ranges.

- When you switch between enabling and disabling these permissions, changes take effect immediately and a service restart in Grid Manager is not required. However, you may need to refresh Grid Manager to view the changes.
- You can assign these permissions when DNS, DHCP, or Microsoft Management licenses are installed. If you remove all of these licenses after you have configured relevant permissions for supported resources, the appliance retains the permissions, but you will not be able to see the permissions nor configure them.

Changes to Default Behavior

This section describes changes to the default behavior when you enable permissions for DNS resources with associated IP addresses in networks and ranges. The following table lists behavior in previous releases and changes made in this release for supported resources. Review these changes before you configure permissions for these resources. For more information about how to define these permissions, see Permissions Examples.

<table>
<thead>
<tr>
<th>Resources</th>
<th>Behavior in Previous NIOS Releases</th>
<th>Changes in NIOS 6.10.4</th>
</tr>
</thead>
</table>
| A Records | Admins can add, modify, and delete A, AAAA, PTR records and DNS hosts that have associated IP addresses in a network or range when they have read/write permission for the respective zone or a higher level DNS parent object (even if they have deny or read-only permission for the network to which the DNS resources belong). | When you enable new permissions, you can define the following permissions for the admins to add, modify, and delete A, AAAA, PTR records and DNS hosts that have associated IP addresses in a network container, network, or range:  
  - Read/write permission for the specific records in the zone or a higher level DNS parent object.  
  - Read/write permission for the records in the specified network container, network, or range to which the resources belong.  
  Note: Fields for A, AAAA, PTR records and DNS hosts in a zone or a higher level DNS parent object, except Name, IP Address, MAC Address, DUID and Disabled, can be modified by admins who do not have write permission for the same records in the specified network container, network, or range.  
  - You cannot define read-only permission for A, AAAA, and PTR records in a range. The read operation for A, AAAA, PTR, and host records is based on DNS permission hierarchy. In other words, read-only permission for a parent DNS zone allows you to view DNS objects, regardless of the permission you have defined for these resources in their associated ranges. |
| DHCP-enabled Hosts | • Admins can add, modify, and delete DHCP-enabled host addresses when they have read/write permission for hosts in the specified zone and read/write permission for the network to which the IP addresses belong. (This behavior stays the same in NIOS 6.10.4.) | • When you enable new permissions and you want to allow the admin to add, modify, and delete DHCP-enabled hosts that fall within a specific address range, define read/write permission for hosts in that specified range. Note that if the admin has read/write permission for the network, they can add, modify, and delete hosts that do not fall within a specific address range. |
| Fixed Addresses/ Reservations | • Admins can add, modify, and delete fixed addresses and reservations in an address range when they have read/write permission for DHCP fixed addresses for the network to which the range belongs. | • When you enable new permissions and you want to allow the admin to add, modify, and delete fixed addresses and reservations in a specific address range, define read/write permission for fixed addresses or reservations in that specified range. Note that if the admin has read/write permission for the network, they can add, modify, and delete fixed addresses and reservations that do not fall within a specific address range. |

**Enabling Permissions for DNS Resources in Networks and Ranges**

To enable permission for DNS Resources in Networks and Ranges:

1. From the **Grid** tab, select the **Grid Manager** tab.
2. Expand the Toolbar and select **Grid Properties -> Edit**.
3. In the **Grid Properties** editor, select the **General** tab -> **Advanced** tab, and then complete the following:
   - **Enable DNS Object Permissions in Networks and Ranges**: Select this check box to enable DNS object permissions in networks and ranges. When you enable this, admins with Read/Write permission for specific records in a zone or a higher-level DNS parent object, and admins with Read/Write permission for resource records in specified network containers, networks, or ranges can add, modify, and delete A, AAAA, PTR records, and DNS hosts that have associated IP addresses in the network containers, networks, or ranges.
4. Save the configuration and click **Restart** if it appears at the top of the screen.

**Configuring Permissions for DNS Resources in Networks and Ranges**

To define permissions for resources that are associated with IP addresses in a network container, network, or address range, complete the following:

1. Log in to the appliance through the Infoblox CLI and use the **set dns_perm_for_nw_range** command to enable new permissions, as follows:
   ```plaintext
   Infoblox > set dns_perm_for_nw_range on
   
   You can also enable permission for DNS resources in networks and ranges through the Infoblox GUI, as described in [Enabling Permissions for DNS Resources in Networks and Ranges](#).
   
2. Log in to Grid Manager and depending on which permission you want to define, do one of the following:
   - **Network View**: From the **Administration** tab, select the **Networks View** tab -> **network_view** check box and click the Edit icon.
   - **Network Container**: From the **Data Management** tab, select the **IPAM** tab -> **network_container** check box and click the Edit icon.
   - **Network**: From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** -> **addr_range** check box, and then click the Edit icon.
   - **DHCP Range**: From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** -> **addr_range** check box, and then click the Edit icon.
   - **Fixed Address**: From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** -> **addr_range** check box, and then click the Edit icon.
fixed_address check box, and then click the Edit icon.

Reservation: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> reservation check box, and then click the Edit icon.

Zone: From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and then click the Edit icon.

Note: You cannot assign permissions for zones that are auto-created.

2. In the editor, click the Permissions tab, and select the supported permission from the Permissions drop-down list for the admin group or role.
3. Select a resource from the drop-down list in the Resources column.
4. Save the configuration.

Permission Examples

The following table lists examples for configuring new permissions for fixed addresses (or reservations) in network 10.1.2.0/24 and range 10.1.2.1-10.1.2.10.

<table>
<thead>
<tr>
<th>Action</th>
<th>Permission for network 10.1.2.0/24</th>
<th>Permission for range 10.1.2.1-10.1.2.10</th>
<th>Action Allowed? (Yes/No)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add, modify, or delete fixed address 10.1.2.5</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Add, modify, or delete fixed address 10.1.2.5</td>
<td>No</td>
<td>Read/write for &quot;Fixed addresses in 10.1.2.1-10.1.2.10 Range&quot;</td>
<td>Yes</td>
<td>Read/write permission at the range level is sufficient for creating a fixed address that falls within the range.</td>
</tr>
<tr>
<td>Add, modify, or delete fixed address 10.1.2.100</td>
<td>Read/write for &quot;Fixed addresses in 10.1.2.0/24 Network&quot;</td>
<td>Deny for &quot;Fixed addresses in 10.1.2.1-10.1.2.10 Range&quot;</td>
<td>Yes</td>
<td>Since fixed address 10.1.2.100 does not belong to the 10.1.2.1-10.1.2.10 range, read/write permission for &quot;Fixed addresses in 10.1.2.0/24 Network&quot; is sufficient for the operation.</td>
</tr>
</tbody>
</table>

The following table lists some examples for configuring DNS resources that have associated IP addresses in a network or range:

<table>
<thead>
<tr>
<th>Action</th>
<th>Permission for DNS zone corp.xyz.com</th>
<th>Permission for network 10.1.2.0/24</th>
<th>Permission for range 10.1.2.1-10.1.2.10</th>
<th>Action Allowed? (Yes/No)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add, modify, or delete an A record with IP address 10.1.2.8</td>
<td>Read/write permission for corp.xyz.com</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Read/write permission for &quot;A Records in 10.1.2.1-10.1.2.10 range&quot; is also required.</td>
</tr>
<tr>
<td>Add, modify, or delete an A record with IP address 10.1.2.8</td>
<td>Read/write permission for corp.xyz.com</td>
<td>No</td>
<td>Read/write for &quot;A Records in 10.1.2.1-10.1.2.10 Range&quot;</td>
<td>Yes</td>
<td>Since 10.1.2.8 falls within the 10.1.2.1-10.1.2.10 range, read/write permission for &quot;A Records in 10.1.2.1-10.1.2.10 Range&quot; and read/write for corp.xyz.com are both required.</td>
</tr>
<tr>
<td>Add, modify, or delete an A record with IP address 10.1.2.8, and modify or delete a network</td>
<td>Read/write permission for corp.xyz.com</td>
<td>Read-only permission for network 10.1.2.0/24</td>
<td>Read/write for &quot;A Records in 10.1.2.1-10.1.2.10 Range&quot;</td>
<td>Yes for A record</td>
<td>Admins can add, modify, and delete A records because they have read/write permissions for the zone and range; but they cannot modify or delete networks because they have read-only permission for network 10.1.2.0/24.</td>
</tr>
<tr>
<td>Add, modify or delete DHCP-enabled host address 10.1.2.22</td>
<td>Yes if the host is a DNS host. N/A if the host is a DHCP host.</td>
<td>Read/write permission for &quot;IPv4 Hosts in 10.1.2.0 network&quot;</td>
<td>No</td>
<td>Yes</td>
<td>Host address 10.1.2.22 is within the 10.1.2.0 network but outside of the 10.1.2.1-10.1.2.10 range, so read/write permission for &quot;IPv4 Hosts in 10.1.2.0 network&quot; is sufficient.</td>
</tr>
<tr>
<td>Add, modify, or delete DHCP-enabled host address 10.1.2.8, and modify or delete a network</td>
<td>Yes if the host is a DNS host. N/A if the host is a DHCP host.</td>
<td>Read-only permission for network 10.1.2.0/24</td>
<td>Read/write for &quot;Hosts in 10.1.2.1-10.1.2.10 Range&quot;</td>
<td>Yes for A record</td>
<td>Admins can add, modify, and delete DHCP-enabled hosts because they have read/write permissions for &quot;Hosts in 10.1.2.1010.1.2.10 range&quot;; but they cannot modify or delete networks because they have read-only permission for network 10.1.2.0/24.</td>
</tr>
</tbody>
</table>
The following table lists an example for permissions required to configure PTR records that have associated IP addresses in a network:

<table>
<thead>
<tr>
<th>Action</th>
<th>Permission for DNS zone corpxyz.com</th>
<th>Permission for network 10.1.2.0/24</th>
<th>Permission for reverse zone 0.0.10.in-addr.arpa</th>
<th>Action Allowed? (Yes/No)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add, modify, or delete a PTR record with IP address 5.0.0.10.</td>
<td>Read/write permission for corpxyz.com</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Read/write permission for “PTR Records in corpxyz.com and 0.0.10.in-addr.arpa” is required.</td>
</tr>
</tbody>
</table>

Administrative Permissions for DHCP Resources

Limited-access admin groups can access certain DHCP resources only if their administrative permissions are defined. By default, the appliance denies access when a limited-access admin group does not have defined permissions. You can grant admin groups read-only or read/write permission, or deny access to the following DHCP resources:

- Network views
- IPv4 networks
- Hosts
- IPv4 DHCP ranges
- IPv4 DHCP fixed addresses
- IPv4 DHCP reservations
- MAC address filters
- IPv4 shared networks
- IPv4 network templates
- IPv4 DHCP range templates
- IPv4 fixed address templates
- IPv4 DHCP enabled host addresses
- IPv4 DHCP lease history
- Roaming hosts
- IPv6 networks
- IPv6 DHCP ranges
- IPv6 DHCP fixed addresses
- IPv6 DHCP enabled host addresses
- IPv6 shared networks
- IPv6 network templates
- IPv6 DHCP range templates
- IPv6 fixed address templates
- IPv6 DHCP lease history

You can grant an admin group broad permissions to DHCP resources, such as read/write permission to all IPv4 or IPv6 networks and shared networks in the database. In addition, you can grant permission to specific resources, such as a specific IPv4 or IPv6 network or DHCP range, or an individual address in an IPv4 or IPv6 network. Permissions at more specific levels override global permissions. You can also define permissions for specific DHCP objects and Grid member to restrict admins to perform only the specified DHCP tasks on the specified member. For more information, see Defining DNS and DHCP Permissions on Grid Members.

The following sections describe the different types of permissions that you can set for DHCP resources:

- 4823706
- 4823706
- 4823706
- 4823706
- 4823706
- 4823706
- 4823706
- 4823706

Administrative Permissions for Network Views

Limited-access admin groups can access network views, including the default network view, only if they have read-only or read/write permission to a specific network view or to all network views. Permissions granted to a network view apply to all its IPv4 and IPv6 networks, shared networks, DHCP ranges and fixed addresses.

You can grant admin groups read-only or read/write permission, or deny access to network views as follows:

- All network views—Global permission that applies to all network views in the database.
- A specific network view—Permission to a specific network view applies to the properties you set in the Network View editor, and to all the
IPv4 and IPv6 networks and shared networks in the network view. This overrides the global permission to all network views. When you configure permissions for a network view, you can also set permissions for the following:

- All IPv4 and IPv6 networks in the selected network view—If you do not define permissions for IPv4 or IPv6 networks, they inherit the permissions of their network view.
- All IPv4 and IPv6 shared networks in a specific network view—If you do not define permissions for IPv4 or IPv6 shared networks, they inherit the permissions of their network view.

Note that you can grant an admin group read-only or read/write permission to specific IPv4 or IPv6 networks in a network view, without granting them permission to that network view. For information, see `4823706 4823706`. For information on how to define permissions for network views, see *Applying Permissions and Managing Overlaps*.

The following table lists the tasks admins can perform and the required permissions for network views.

**Table 4.18 Network View Permissions**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All DNS Views</th>
<th>Specific DNS View</th>
<th>All Network Views</th>
<th>Specific Network View</th>
<th>All IPv4 or IPv6 Networks</th>
<th>All IPv4 or IPv6 Shared Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and delete network views and their associated DNS views</td>
<td>RW</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create and delete a network view and its associated DNS views</td>
<td>RW</td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 and IPv6 networks and shared networks in all network views</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 and IPv6 networks and shared networks in a network view</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View the properties of all network views</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View network statistics of all network views</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for all IPv4 and IPv6 networks and shared networks</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View the properties of a network view</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for IPv4 and IPv6 networks and shared networks in a network view</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expand and join IPv4 and IPv6 networks</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expand and join IPv4 and IPv6 networks in a specific network view</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Create, modify, and delete IPv4 and IPv6 networks, DHCP ranges and fixed addresses in a specific network view

View network statistics and properties of all networks in a network view

Search for IPv4 and IPv6 networks in a network view

Create, modify, and delete all IPv4 or IPv6 shared networks

View the properties of all IPv4 or IPv6 shared networks

View and search for IPv4 and IPv6 shared networks in a network view

Restart services from the DHCP tab

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member (s)</th>
<th>All IPv4 or IPv6 Networks</th>
<th>Specific IPv4 or IPv6 Network</th>
<th>All IPv4 or IPv6 Shared Networks</th>
<th>Specific DNS Zone</th>
<th>All IPv4 or IPv6 DHCP Ranges</th>
<th>All IPv4 or IPv6 Fixed Addresses</th>
<th>IPv4 or IPv6 Network Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 networks, DHCP ranges, and fixed addresses without assigned Grid members</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Administrative Permissions for IPv4 and IPv6 Networks and Shared Networks

Limited-access admin groups can access IPv4 and IPv6 networks, including shared networks, only if their administrative permissions are defined. Permissions for a network apply to all its DHCP ranges and fixed addresses. To override network-level permissions, you must define permissions for specific DHCP ranges and fixed addresses. For example, you can grant an admin group read-only permission to a network, read/write permission to its DHCP ranges, and read-only permission to its fixed addresses.

You can grant read-only or read/write permission, or deny access to networks, as follows:

- All IPv4 or IPv6 networks—Global permission that applies to all IPv4 or all IPv6 networks in the database.
- All IPv4 or IPv6 shared networks—Global permission that applies to all IPv4 or all IPv6 shared networks in the database.
- A specific IPv4 or IPv6 network—Network permissions apply to its properties and to all DHCP ranges, fixed addresses and hosts in the network, if they do not have permissions defined. This overrides global permissions.
- All IPv4 or IPv6 DHCP ranges in a network—if you do not define permissions for DHCP ranges, they inherit the permissions of the network in which they reside.
- All IPv4 or IPv6 fixed addresses in a network—if you do not define permissions for fixed addresses, they inherit the permissions of the network in which they reside.

To define permissions for a specific IPv4 or IPv6 network and its DHCP ranges and fixed addresses, see Applying Permissions and Managing Overlaps.

The following table lists the tasks admins can perform and the required permissions for IPv4 and IPv6 networks.

Table 4.19 Network Permissions
<table>
<thead>
<tr>
<th>Action</th>
<th>Read</th>
<th>Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 networks, DHCP ranges, and fixed addresses with assigned Grid members</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Assign a Grid member to a specific IPv4 or IPv6 network and its DHCP ranges</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Expand and join IPv4 or IPv6 networks</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Create IPv4 or IPv6 networks from templates</td>
<td>RW</td>
<td>RO</td>
</tr>
<tr>
<td>Create, modify, and delete an IPv4 or IPv6 network</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>View IPv4 or IPv6 network properties and statistics, and search for DHCP ranges and fixed addresses in a specific network</td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 DHCP ranges and fixed addresses in a specific network</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Create and split an IPv4 or IPv6 network and automatically create a reverse DNS zone</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 shared networks</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>View IPv4 or IPv6 shared networks</td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 DHCP ranges with an assigned member in a specific network</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 DHCP ranges</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>View and search for IPv4 or IPv6 DHCP ranges in a specific network</td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 fixed addresses</td>
<td>RW</td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for IPv4 or IPv6 Fixed Addresses and IPv4 Reservations

IPv4 and IPv6 fixed addresses and IPv4 reservations inherit the permissions of the networks in which they reside. You can override network-level permissions by defining permissions for fixed addresses.

You can grant read-only or read-write permission, or deny access to fixed addresses, as follows:

- All IPv4 fixed addresses/reservations—Global permission that applies to all IPv4 fixed addresses and reservations in the database.
- All IPv6 fixed addresses—Global permission that applies to all IPv6 fixed addresses in the database.
- All IPv4 fixed addresses/reservations in a network—Permissions at this level override global permissions. If you do not define permissions for fixed addresses and reservations, they inherit the permissions of the network in which they reside.
- All IPv6 fixed addresses in a network—Permissions at this level override global permissions. If you do not define permissions for IPv6 fixed addresses, they inherit the permissions of the network in which they reside.
- A single IPv4 fixed address/reservation—Overrides global and network-level permissions.
- A single IPv6 fixed address—Overrides global and network-level permissions.

For information on setting permissions for fixed addresses, see Applying Permissions and Managing Overlaps.

The following table lists the tasks admins can perform and the required permissions for IPv4 and IPv6 fixed addresses.

Table 4.20 Permissions for Fixed Addresses/Reservations

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Specific IPv4 or IPv6 Network</th>
<th>All IPv4 or IPv6 fixed Addresses/IPv4 Reservations</th>
<th>Specific IPv4 or IPv6 Fixed Address/IPv4 Reservation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete IPv4 fixed addresses/reservations or IPv6 fixed addresses</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 fixed addresses/reservations or IPv6 fixed addresses in a specific network</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete an IPv4 fixed address/reservation or IPv6 fixed address</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for all IPv4 fixed addresses/reservations or IPv6 fixed addresses</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for IPv4 fixed addresses/reservations or IPv6 fixed addresses in a network</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View and search for an IPv4 fixed address/reservation or IPv6 fixed address</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Administrative Permissions for IPv4 or IPv6 DHCP Enabled Host Addresses

A read-write permission to IPv4 or IPv6 Host Address gives limited-access users the ability to create, modify, and delete IPv4 and IPv6 DHCP enabled host addresses in a specified network. Admin users with a read-write permission can create, modify, and delete IPv4 or IPv6 DHCP enabled host addresses only in the specified network. They do not have the ability to create, modify or delete any networks or objects, such as fixed addresses, in those networks.

You can also grant admin users read-only permission or deny access to the following:

- IPv4 Host Address—Object permission that applies to all IPv4 DHCP enabled host addresses in a specified network.
- IPv6 Host Address—Object permission that applies to all IPv6 DHCP enabled host addresses in a specified network.

For information about setting permissions for DHCP enabled host addresses, see Applying Permissions and Managing Overlaps.

The following table lists tasks that admins can perform and the required permissions for IPv4 and IPv6 DHCP enabled host addresses.

Table 4.21 Permissions for DHCP Enabled Host Addresses
### Tasks

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Specific IPv4 or IPv6 Network</th>
<th>All IPv4 or IPv6 DHCP enabled host Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 DHCP enabled host addresses in a specified network</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Modify and delete a specific IPv4 or IPv6 DHCP enabled host address</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>View and search for all IPv4 or IPv6 DHCP enabled host addresses</td>
<td>RO</td>
<td>RO</td>
</tr>
<tr>
<td>View and search for IPv4 or IPv6 DHCP enabled host addresses in a specified network</td>
<td>RO</td>
<td>RO</td>
</tr>
</tbody>
</table>

### Administrative Permissions for IPv4 and IPv6 DHCP Ranges

DHCP ranges inherit the permissions of the networks in which they reside. You can override network-level permissions by defining permissions for DHCP ranges. You can read-only or read/write permission, or deny access to DHCP address ranges, as follows:

- All IPv4 or IPv6 DHCP ranges—Global permission that applies to all IPv4 or IPv6 DHCP ranges in the database.
- All IPv4 or IPv6 DHCP ranges in a network—Permissions at this level override global permissions. If you do not define permissions for DHCP ranges, they inherit the permissions of the network in which they reside.
- A single IPv4 or IPv6 DHCP range—Overides global and network-level permissions.

For information on setting permissions for DHCP ranges, see [Applying Permissions and Managing Overlaps](#). The following table lists the tasks admin can perform and the required permissions for DHCP ranges.

**Table 4.22 DHCP Ranges**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member(s)</th>
<th>Specific IPv4 or IPv6 Network</th>
<th>All DHCP IPv4 or IPv6 Ranges</th>
<th>Specific IPv4 or IPv6 DHCP Range</th>
<th>MAC Address Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 DHCP ranges with an assigned member or a failover association</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete IPv4 or IPv6 DHCP ranges in a network with assigned members</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Modify and delete an IPv4 or IPv6 DHCP range with an assigned member</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>View and search for all IPv4 or IPv6 DHCP ranges with an assigned member</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>View and search for IPv4 or IPv6 DHCP ranges in a network with assigned members</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>View and search for an IPv4 or IPv6 DHCP range with an assigned member</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td></td>
</tr>
</tbody>
</table>
Administrative Permissions for IPv4 or IPv6 DHCP Templates

There are three types of DHCP templates for IPv4 and IPv6 objects—network, DHCP range, and fixed address/reservation templates. To access any of these templates, a limited-access admin group must have read-only permission to the template. Limited-access admin groups cannot have read/write permission to the templates. Only superusers can create, modify and delete network, DHCP range, and fixed address templates. An admin group with read-only permission to the DHCP templates can view them and use them to create networks, DHCP ranges and fixed addresses, as long as they have read/write permissions to those DHCP resources as well.

You can set global read-only permission that applies to all DHCP templates, and you can set permissions to specific templates as well.

For information on setting permissions, see Applying Permissions and Managing Overlaps. The following table lists the tasks admins can perform and the required permissions for DHCP templates.

Table 4.23 Permissions for DHCP Templates

<table>
<thead>
<tr>
<th>Tasks</th>
<th>IPv4 or IPv6 DHCP Templates</th>
<th>All IPv4 or IPv6 Networks</th>
<th>All IPv4 or IPv6 DHCP Ranges</th>
<th>All IPv4 or IPv6 Fixed Addresses/IPv4 Reservations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create IPv4 or IPv6 networks from templates</td>
<td>RO</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create IPv4 or IPv6 DHCP ranges from templates</td>
<td>RO</td>
<td></td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Create IPv4 fixed addresses/reservations or IPv6 fixed addresses from templates</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View templates</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note the following additional guidelines:

- DHCP range templates and fixed address templates do not inherit their permissions from network templates. You must set permissions for each type of template.
- An admin group can create a network using a network template that includes a DHCP range template and a fixed address template, even if it has no permission to access the DHCP range and fixed address templates.

Administrative Permissions for Roaming Hosts

Limited-access admin groups can access roaming hosts only if their administrative permissions are defined. The appliance denies access to roaming hosts for which an admin group does not have defined permissions.

You can grant read-only or read/write permission, or deny access to roaming hosts as follows:

- All roaming hosts in the database—Global permission that applies to all the roaming hosts in the database.
- A specific roaming host—Permissions that applies to specific roaming host.

For information on setting permissions, see Applying Permissions and Managing Overlaps. The following table lists the tasks admins can perform and the required permissions for roaming host.

Table 4.24 Permissions for Roaming Hosts

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid DHCP Properties</th>
<th>Specific IPv4 or IPv6 Roaming Host</th>
<th>All Roaming Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable roaming hosts</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View roaming host</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
</tr>
<tr>
<td>Create, modify, and delete roaming hosts</td>
<td>RO</td>
<td></td>
<td>RW</td>
</tr>
<tr>
<td>Modify and delete roaming host</td>
<td>RO</td>
<td></td>
<td>RW</td>
</tr>
</tbody>
</table>
Administrative Permissions for MAC Address Filters
Limited-access admin groups can access MAC address filters only if their administrative permissions are defined. The appliance denies access to MAC address filters for which an admin group does not have defined permissions.
You can grant read-only or read/write permission, or deny access to MAC address filters as follows:

- All MAC address filters in the database
- A specific MAC address filter

For information on setting permissions, see Applying Permissions and Managing Overlaps. The following table lists the tasks admins can perform and the required permissions for MAC address filters.

**Table 4.25 Permissions for MAC Filters**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>All MAC Address Filters</th>
<th>Specific MAC Address Filter</th>
<th>Specific IPv4 DHCP Ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create, modify, and delete MAC address filters</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create, modify, and delete MAC address entries for a MAC address filter</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify and delete a MAC address filter</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply a MAC address filter to an IPv4 DHCP range</td>
<td>RO</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Delete a MAC address filter from an IPv4 DHCP range</td>
<td>RO</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>View MAC address filters and their MAC address entries</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View a MAC address filter and its MAC address entries</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Administrative Permissions for the IPv4 and IPv6 DHCP Lease Histories
A limited-access admin group can view and export the IPv4 and IPv6 DHCP lease histories if it has read-only permission to the IPv4 and IPv6 DHCP lease history. Permissions to the IPv4 and IPv6 DHCP lease histories are different from the network permissions. Therefore, an admin group can access the IPv4 and IPv6 DHCP lease histories, regardless of its network permissions. Note that only superusers can import a DHCP lease history file.

To define permissions for the IPv4 and IPv6 DHCP lease histories:

1. For an admin group: From the Administration tab, select the Administrators tab -> Permissions tab -> admin_group in the Groups table, and then click the Add icon -> Global Permissions from the Create New Permission area or select Add -> Global Permissions from the Toolbar.
   
   or

   For an admin role: From the Administration tab, select the Administrators tab -> Permissions tab -> admin_role in the Roles table, and then click Add icon -> Global Permissions from the Create New Permission area or select Add -> Global Permissions from the Toolbar.

2. Complete the following in the Manage Global Permissions dialog box:
   - **Permission Type:** Select DHCP Permissions from the drop-down list.
   - In the table, select Read/Write, Read-only, or Deny for All IPv4 DHCP Lease History and All IPv6 DHCP Lease History.

3. Save the configuration and click Restart if it appears at the top of the screen.

Administrative Permissions for File Distribution Services
You can restrict access to the TFTP, HTTP and FTP services provided by the appliance. By default, the appliance denies access to the TFTP, HTTP and FTP services, unless an admin group has their administrative permissions defined.

You can grant read-only or read/write permission, or deny access to the following resources:

- Grid File Distribution Properties—Applies to the Grid and its members, directories, and files. You can set this from the Administrators perspective only.
- Member File Distribution Properties—Applies to the Grid member properties only.
- A specific directory—Applies to the directory and its files.

For information on setting permissions, see Applying Permissions and Managing Overlaps. The following table lists the tasks admins can perform and the required permissions for file distribution services.

**Table 4.26 Permissions for File Distribution Services**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid File Distribution Properties</th>
<th>Member Distribution Properties</th>
<th>Specific Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasks</td>
<td>All Dashboard Tasks</td>
<td>Add Networks</td>
<td>Add Hosts</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------</td>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Configure all tasks in the IPAM task pack</td>
<td>RO RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the Add Networks task</td>
<td>RO RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the Add Hosts task</td>
<td>RO RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the Add Fixed Addresses task</td>
<td>RO RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the Add CNAME Record task</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the Add TXT Record task</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the Add MX Record task</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Administrative Permissions for Dashboard Tasks**

Limited-access admin groups can configure IPAM tasks on the Tasks Dashboard only if their administrative permissions are defined. The appliance denies access to IPAM tasks for which an admin group does not have defined permissions.

You can grant read-only or read/write permission, or deny access to IPAM tasks as follows:

- All IPAM tasks on the Tasks Dashboard
- A specific IPAM task

When you deny access to an IPAM task for an admin group, users cannot configure the task on their dashboards. Users must have at least read-only permission to a specific task to see it in the task pack. To perform a specific task, users must also have read/write permission to the objects associated with the task. For information about specific permissions for IPAM, DNS, and DHCP objects, see *Administrative Permissions for IPAM Resources, Administrative Permissions for DNS Resources, and Administrative Permissions for DHCP Resources.*

For information about setting permissions, see *Applying Permissions and Managing Overlaps.* The following table lists the tasks admins can perform and the required permissions for configuring IPAM tasks on the Tasks Dashboard.

*Table 4.27 Permissions for IPAM Tasks*

**Administrative Permissions for Certificate Authentication Services and CA Certificates**

Limited-access admins can configure certificate authentication services and CA certificates only if their administrative roles and permissions are defined. If you want to allow admins to configure two-factor authentication, you can assign the PKI Admin role to limited-access admins or grant them read/write permissions to the following:

- All certificate authentication services
- All CA Certificates

For information about setting permissions, see *Applying Permissions and Managing Overlaps.* The following table lists the admin tasks and required permissions for configuring certificate authentication services and managing CA certificates.
### Administrative Permissions for Object Change Tracking

Infoblox stores updated objects in the NIOS database. Users with read-only permission can query and view these objects. Grid Manager allows you to grant the following permissions:

- Read-only permission to view deleted objects information. If the users have a read-only permission and the `exclude_deleted` flag is not set, then they will receive information about the deleted objects only.
- Deny to prevent the users from accessing updated objects information. If the users have a Deny permission, then they cannot query for any object updates even if the `exclude_deleted` flag is not set.

Users with a read-only permission must have permissions on all the objects to perform a full or an incremental synchronization. For example, consider that a user, user1, has read-only permission on DNS views, but does not have permission on network views. If user1 performs a full synchronization, NIOS does not include network views in the response as user1 does not have permission to view these objects. Hence, Infoblox recommends that you give permissions to all the objects in the NIOS database.

### Administrative Permissions for Load Balancers

Limited-access admins can view and manage GLBs (Global Load Balancers), load balancer synchronization groups, and their associated objects if their administrative roles and permissions are defined. If you want to allow admins to manage GLB objects, assign the Load Balancer Admin role to limited-access admins and grant them the following permissions:

- Read/write, read-only, or deny permission to NIOS managed GLB groups and independent load balancers
- Read/write, read-only, or deny permission to NIOS managed GLB objects
- Read-only or deny permission to GLB objects, such as DNS profiles and iRules, that are synchronized from the GLB but cannot be managed through NIOS

For information about setting permissions, see *Applying Permissions and Managing Overlaps*. The following table lists the admin tasks and required permissions for configuring GLBs, load balancer synchronization groups, and their associated objects.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member(s)</th>
<th>All Load Balancer Objects</th>
<th>All Load Balancers</th>
<th>All Load Balancer Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>View load balancer objects</td>
<td>RO</td>
<td>RO</td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>Add and modify synchronized load balancer objects</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Add, modify, and delete synchronized load balancer objects</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Modify and delete synchronized load balancer groups</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td></td>
</tr>
</tbody>
</table>

### Administrative Permissions for Named ACLs

Only superusers and limited-access users with Read/Write permission to All Named ACLs and Read/Write permission to the corresponding objects and operations can manage named ACLs and their ACEs.

For information about access control and named ACLs, see *Configuring Access Control*. The following table lists the operations and required permissions for managing named ACLs.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Member(s)</th>
<th>All Load Balancer Objects</th>
<th>All Load Balancers</th>
<th>All Load Balancer Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Create, modify, and delete named ACLs for all supported operations

View named ACLs and ACEs

### Administrative Permissions for DNS Threat Protection

You can grant read-only or read/write permission, or deny access to the following resources:

- Grid Security Properties—Applies to the Grid and its members.
- Member Security Properties—Applies to the Grid members only.

For information about setting permissions, see Applying Permissions and Managing Overlaps. The following table lists the tasks admins can perform and the required permissions for the threat protection service.

#### Table 4.31 Permissions for hardware-based Threat Protection Service

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Security Properties</th>
<th>Member Security Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Grid security properties</td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>Update Grid Security properties</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>View member security properties for specific Grid members</td>
<td>RO</td>
<td>RO</td>
</tr>
<tr>
<td>Update member security properties for specific Grid members</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Start and stop threat protection service for a Grid member</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Publish rules for a Grid member</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>View rule categories and rules for the Grid</td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>Enable and disable rules for the Grid</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Update rule versions for any rules on the Grid</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Revert to a previous rule version for any rules on the Grid</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Modify configuration parameters, such as action and severity, for rules on the Grid</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Create custom rules from rule templates for the Grid</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>Delete custom rules for the Grid</td>
<td>RW</td>
<td></td>
</tr>
<tr>
<td>View rule categories and rules on a Grid member</td>
<td>RO</td>
<td>RO</td>
</tr>
<tr>
<td>Enable and disable rules on a Grid member</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Update rule versions for any rules on a Grid member</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Revert to a previous rule version for any rules on a Grid member</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Modify configuration parameters, such as action and severity, for rules on a Grid member</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>View threat protection related event statistics on a Grid member</td>
<td>RO</td>
<td>RO</td>
</tr>
<tr>
<td>Upgrade rulesets for a Grid</td>
<td>RW</td>
<td></td>
</tr>
</tbody>
</table>

#### Table 4.32 Permissions for Software ADP

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Security Properties</th>
<th>Member Security Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the list of Threat Protection profiles in the Profiles Viewer</td>
<td>RO</td>
<td>RO</td>
</tr>
<tr>
<td>View profile settings in the Threat Protection Profile Editor</td>
<td>RO</td>
<td></td>
</tr>
</tbody>
</table>
Create a Threat Protection profile

Clone a Threat Protection profile from an existing profile (This also clones all settings for the ruleset from an old profile.)

Clone a Threat Protection profile from an existing member settings

Update the profile settings (name, comment, events per second, disable multiple TCP DNS request, list of members)

Change the ruleset that is assigned to a profile (This internally merges all customizations for an old ruleset to a new ruleset.)

View the profile rules and rule settings

Enable/disable rules in the profile

Change the rule parameters for rules in the profile (action, log severity, events per second etc.)

Merge two profiles

Assign/remove a profile from Member Security properties

Delete a profile

Administrative Permissions for DNS Threat Analytics

Only superusers and limited-access users with Read/Write permission can manage Threat Analytics service. You can grant read-only or read/write permission, or deny access to the following:

- Grid Threat Analytics Properties—Applies to the Grid and its members.

For information about setting permissions, Managing Permissions. The following table lists the tasks admins can perform and the required permissions for the threat analytics service.

Table 4.33 Permissions for Threat Analytics Service

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Grid Threat Analytics Properties</th>
<th>RPZ Zones</th>
<th>Grid Members</th>
<th>DNS Views</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Grid Threat Analytics properties</td>
<td>RO</td>
<td>RO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Threat Analytics properties</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Start and stop Threat Analytics service</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create an RPZ and use it as mitigation blacklist feed</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>View whitelisted domains</td>
<td>RO</td>
<td></td>
<td>RO</td>
<td></td>
</tr>
<tr>
<td>Move blacklisted domains to the whitelist</td>
<td>RW</td>
<td>RW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Threat Analytics module and whitelist sets</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Viewing threat analytics module and whitelist versions</td>
<td>RO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define the Threat Analytics Update policy</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manually Upload Threat Analytics Updates</td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Administrative Permissions for All Rulesets

You can grant permissions for individual ruleset objects to admin users. NIOS provides a global permission ALL Rulesets for admin groups. To perform operations on an NXDOMAIN ruleset, a blacklist rule, or an RPZ ruleset, you must have permission to the rule or ruleset to which the ruleset object belongs.

Administrative Permissions for Cloud Objects

You can grant read-only or read/write permission, or deny access to the following cloud related objects:

- All tenant—Applies to all tenants.
- Per tenant object—Applies to selected tenants only.

You need appropriate permissions to make changes to all tenants or a specific tenant object through Grid Manager. Note that following:

- Update the tenant object: You must have permission on all tenant objects or the specific tenant object that is being updated. When you
modify any tenant object associated with a tenant, it requires explicit Read/Write permission on the specific tenant object, whether permission on the associated tenant exists or not.

- Read-Only: This operation returns all tenant objects if you have the all tenant permission, or returns only specific tenant objects for which you have access.
- Permission for a tenant object implicitly gives the read permission to any object that is associated with the tenant.
- Note that creating and deletion operations do not need any permission.

### Administrative Permissions for CSV Import

The following CSV import permissions are applicable to local users on the NIOS appliance. They are not valid for AD or RADIUS users.

- When you delete a user, CSV import tasks associated with the respective user are not deleted. Superusers can access these tasks. Pending CSV import tasks will not be executed due to authentication failure.
- If you change user permissions, the pending and running CSV import tasks are executed, but may finish with errors. Note that the appliance re-establishes database transaction after every 500 lines are imported. If you delete or modify the respective user entry between these transactions, the rest of the import may fail.
- Superusers can manage any stopped, failed, or completed CSV import tasks belonging to a deleted user.

### Administrative Permissions for Reporting

NIOS supports global and object permissions for reporting: Reports and Searches. Consider the following when applying permissions for reports and searches:

- When you view a DNS report, DHCP report, or search options, you can view all the data in the corresponding report or search results, even if you do not have permissions to view the DNS or DHCP objects.
- A limited-access user needs relevant permissions to view any report or search.
- When you grant a read-only permission for a specific report to a user, the user receives read-only access to everything the report displays.
- A user can view report data returned by a search operation even when the user is denied access to the search operation.
- You can only view pre-defined reports, global reports and customized reports or searches. A user, including superuser, cannot view customized reports or searches of other users.
- You cannot edit pre-defined reports.
- Only a superuser can edit global reports or searches.
- Only an owner of the customized report or search operation can modify the report.
- Superuser may create reports up to system wide limit.
- A limited-access admin can create up to five reports by default. You can configure this limitation through Grid Manager.

### Chapter 5 Deploying a Grid

To deploy a Grid, it is important to understand what a Grid is, how to create a Grid Master and add members, and how to manage the Grid. This chapter explains these tasks in the following sections:

- Introduction to Grids
  - Grid Communications
  - NAT Groups
  - Automatic Software Version Coordination
  - Grid Bandwidth Considerations
- About HA Pairs
  - Planning for an HA Pair
  - About HA Failover
  - VRRP Advertisements
- Creating a Grid Master
  - Port Numbers for Grid Communication
  - Grid Setup Wizard
  - Creating an HA Grid Master
  - Creating a Single Grid Master
- Adding Grid Members
  - Adding a Single Member
  - Adding an HA Member
  - Changing the Communication Protocol for a Dual Mode Appliance
  - Joining Appliances to the Grid
  - Grouping Members by Extensible Attributes
- Configuring an IPv6-only Grid
  - Transforming to an IPv6-only Grid
- Auto-Provisioning NIOS Appliances
  - Joining Auto-Provisioned Appliances to the Grid
- Pre-Provisioning NIOS and vNIOS Appliances
  - Guidelines for Pre-provisioning Offline Grid Members
  - Configuring Pre-Provisioned Members
  - About Provisional Licenses
  - Guidelines for Joining Pre-Provisioned Members to the Grid
- Configuration Example: Configuring a Grid
Introduction to Grids

A Grid is a group of two or more NIOS appliances that share sections of a common, distributed, built-in database and which you configure and monitor through a single, secure point of access: the Grid Master. A Grid can include Infoblox appliances and vNIOS appliances. A vNIOS appliance is a non-Infoblox hardware platform running the vNIOS software package. For supported vNIOS platforms, see Supported vNIOS Appliance Models and Specifications.

Infoblox appliances support both IPv4 and IPv6 networks and you can configure a Grid in one of the following modes:

- **IPv4-only**: An IPv4-only Grid uses IPv4 as the Grid communication protocol and it includes an IPv4 Grid Master and the Grid members, which can be either IPv4 or dual mode (IPv4 and IPv6) independent and HA appliances. Note that when you add a dual mode HA member to an IPv4-only Grid, the communication protocol between the two nodes of an HA pair must be IPv4.
- **IPv6-only**: An IPv6-only Grid uses IPv6 as the Grid communication protocol and it includes an IPv6 Grid Master and the Grid members, which can be either IPv6 or dual mode (IPv4 and IPv6) independent and HA appliances. Note that when you add a dual mode HA member to an IPv6-only Grid, the communication protocol between the two nodes of an HA pair must be IPv6.
- **IPv4 and IPv6 (Dual mode)**: A dual mode Grid can use either IPv4 or IPv6 as the Grid communication protocol. A dual mode Grid includes a dual mode Grid Master and the Grid members, which can be either IPv4, IPv6, or dual mode independent and HA appliances.

Note: Infoblox appliances support IPv4 and IPv6 networking configurations in most deployments cited in this chapter. You can set the LAN1 port to an IPv6 address and use that address to access Grid Manager. All HA (high availability) operations can be applied across IPv6. Topics in this and following chapters generally use IPv4 examples. Also note that the LAN2, MGMT, and VLAN ports also support IPv6. DNS services are fully supported in IPv6 for the LAN1, LAN2, MGMT, and VLAN ports. DHCP services are fully supported in IPv6 for the LAN1 and LAN2 ports. Examples throughout this chapter use IPv4 addressing. Interfaces on NIOS appliances support both IPv4 and IPv6 transports and intra-Grid communication is based on the type of IP address used by the Grid member to join the Grid.

The following table summarizes the possible setups of a Grid configuration:

<table>
<thead>
<tr>
<th>Grid Configuration</th>
<th>VRRP Protocol for HA Pair</th>
<th>Grid Communication Protocol</th>
<th>Grid Connection via MGMT</th>
<th>Additional IPv4 Addresses</th>
<th>Additional IPv6 Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Grid Master</td>
<td>IPv4</td>
<td>IPv4</td>
<td>NA</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPv6 Grid Master</td>
<td>IPv6</td>
<td>IPv6</td>
<td>NA</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dual mode Grid Master</td>
<td>IPv4 or IPv6</td>
<td>IPv4 or IPv6</td>
<td>NA</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPv4 Grid member</td>
<td>IPv4</td>
<td>IPv4</td>
<td>IPv4</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPv6 Grid member</td>
<td>IPv6</td>
<td>IPv6</td>
<td>IPv6</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dual mode Grid member</td>
<td>IPv4 or IPv6</td>
<td>IPv4 or IPv6</td>
<td>IPv4 or IPv6</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

You can also add supported Reporting platforms as a logging and reporting devices in your Grid. Infoblox provides a few Infoblox platforms that you can use as the logging and reporting device. For information about the supported appliances, see About Reporting Clustering. Infoblox reporting solution supports both IPv4 and IPv6 networks and you can configure a reporting member in either IPv4, IPv6, or in dual mode (IPv4 and IPv6) network environment. An IPv4-only Grid uses IPv4 as the Grid communication protocol, so you can add an IPv4 or dual mode reporting member to an IPv4-only Grid. An IPv6-only Grid uses IPv6 as the Grid communication protocol, so you can add an IPv6 or dual mode reporting member to an IPv6-only Grid. However, a dual mode Grid can use either IPv4 or IPv6 as the Grid communication protocol, so you can add an IPv4, IPv6, or a dual mode reporting member to a dual mode Grid. The reporting appliance collects data from members in the Grid and stores the data in the database. It then uses the data to generate predefined and user-defined reports that you can access through Grid Manager. These reports provide useful information about the IPAM, DNS, DHCP, and system activities and usage in your Grid. For more information about reporting, see Infoblox Reporting and Analytics.
Instead of manually provisioning IP addresses and DNS name spaces for network devices and interfaces, you can add Cloud Platform Appliances to leverage DNS and DHCP features of the Grid to manage your CMPs (Cloud ManagementPlatforms). For information about the Infoblox Cloud Network Automation solution and supported Grid configurations, see Deploying Cloud Network Automation.

Figure 5.1 shows the basic concept of a Grid, database distribution (or "replication"), and reporting.

**Figure 5.1 Grid and Partitioned Database Replication**

![Diagram of Grid and Database Replication](image)

The Grid Master can be either an HA master or a single master; that is, an HA (high availability) pair or a single appliance. Similarly, a Grid member can be either a single member or an HA member. You can add single appliances and HA pairs to a Grid, forming single members and HA members respectively. A single Grid member can be either an Infoblox appliance or a vNIOS appliance. An HA Grid member can be a pair of Infoblox appliances or vNIOS appliances. For information, see Supported vNIOS Appliance Models and Specifications.

The Grid Master communicates with every Grid member in a hub-and-spoke configuration. Intra-Grid communication is based on the type of IP address used by the Grid member to join the Grid Master. An IPv4-only Grid Master uses IPv4 and an IPv6-only Grid Master uses IPv6 for intra-Grid communication. However, a dual mode Grid Master uses either IPv4 or IPv6 depending on the IP address type used by the Grid member to join the Grid Master. For an HA member, the Grid Master communicates with the active node, which in turn communicates with the passive node, as shown in Figure 5.2.

**Figure 5.2 Grid Communications to an HA Member**

![Diagram of Grid Communications to an HA Member](image)

When adding vNIOS appliances to a Grid, you centralize the management of core network services of the virtual appliances through the Grid Master. vNIOS appliances support most of the features of the Infoblox NIOS software, with some limitations as described in Appendix E, “vNIOS Appliances”.

For additional information specific to each platform, refer to the Quick Start Guide for Installing vNIOS Software on Riverbed Services Platforms a...
By default, Grid communications use the UDP transport with a source and destination port of 1194. This port number is configurable. For a port change to take effect, one of the following must occur: the HA master fails over, the single master reboots, or the Grid restarts services. After adding an appliance or HA pair to a Grid, you no longer access the Infoblox GUI on that appliance. Instead, you access the GUI running on the Grid Master. Although you can create multiple administrator accounts to manage different services on various Grid members, all administrative access is through the Grid Master. So even if someone has administrative privileges to a single Grid member, that administrator must access the GUI running on the Grid Master to manage that member.

You can access the Infoblox GUI through an HTTPS connection to one of the following IP addresses and ports on the Grid Master:

- The VIP address, which links to the HA port on the active node of an HA Grid Master
- The IP address of the LAN1 port on a single Grid Master
- The IP address of the MGMT port (if enabled) of the active node of an HA or single Grid Master. See Using the MGMT Port.

### Grid Communications

The Grid Master synchronizes data among all Grid members through encrypted VPN tunnels. The default source and destination UDP port number for VPN tunnels is 1194. You can continue using the default port number or change it. For example, if you have multiple Grids, you might want each Grid to use a different port so that you can set different firewall rules for each. Whatever port number you choose to use for the VPN tunnels in a Grid, all the tunnels in that Grid use that single port number.

Before an appliance or HA pair forms a tunnel with the master, they first authenticate each other using the Challenge-Response Authentication Mechanism (CRAM). The source and destination port number for this traffic is 2114. During the CRAM handshake, the master tells the appliance or HA pair what port number to use when building the subsequent VPN tunnel.

*Figure 5.3 VPN Tunnels within a Grid*

Another type of traffic, which flows outside the tunnels, is the VRRP (Virtual Router Redundancy Protocol) advertisements that pass between the active and passive nodes in an HA pair. The VRRP advertisements act like heartbeats that convey the status of each node in an HA pair. If the active node fails, the passive node becomes active. The VIP (virtual IP) address for that pair then shifts from the previously active node to the currently active node.

### NAT Groups

*Note:* Infoblox NAT and NAT groups do not support NAT IPv6 operation.
NAT groups are necessary if the Grid Master is behind a NAT appliance and there are members on both sides of that NAT appliance. Any members on the same side as the master go into the same NAT group as the master and use their interface addresses for Grid communications with each other. Grid members on the other side of that NAT appliance do not go in the same NAT group as the master and use the master's NAT address for Grid communications. These other members outside the NAT appliance can—but do not always need to be—in a different NAT group. To see when NAT groups become necessary for Grid communications, compare Figure 5.4 below with Figure 5.5 and Figure 5.6.

**Figure 5.4 NAT without NAT Groups**

![Diagram of NAT without NAT Groups]

Note: A single or HA member using its MGMT port for Grid communications cannot be separated from the Grid Master behind a NAT appliance. For more information, see *Using the MGMT Port*.

**Figure 5.5 Grid Master in NAT Group**

![Diagram of Grid Master in NAT Group]
The same use of NAT groups that applies to a Grid Master also applies to Master Candidates. If there are no other members behind the same NAT appliance as a Master Candidate, then the Master Candidate does not need to be in a NAT group. It always uses its NAT address for Grid communications. If another member is behind the same NAT appliance as the Master Candidate, then both the candidate and that member need to be in the same NAT group so that—if the candidate becomes master—they can use their interface addresses to communicate with each other (see Figure 5.6).

Figure 5.6 Grid Master and Master Candidate in NAT Groups

Although some members might not need to be in a NAT group, it is good practice to put all members in NAT groups in anticipation of adding or rearranging Grid members within the network. For example, in Figure 5.4 – Figure 5.6, Member 4 did not need to be in a NAT group until it became configured as a Master Candidate in bookmark596. At that point, because Member 5 is also behind the same NAT appliance, it became...
necessary to create NAT Group 2 and add Members 4 and 5 to it. Similarly, if you add another member behind the NAT appliance in front of Member 3, then you must create a new NAT group and add Member 3 and the new member to it. Always using NAT groups can simplify such changes to the Grid and ensure that NAT appliances never interrupt Grid communications.

To create a NAT group:

1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and select Grid Properties -> Edit.
3. In the Grid Properties editor, select the NAT Groups tab.
4. Click the Add icon, and enter a name in the Name field and optionally, a comment in the Comment field.
5. Save the configuration and click Restart if it appears at the top of the screen.

To add members to the NAT group:

1. From the Grid tab, select the Grid Manager tab -> Members tab.
2. Select a Grid member and click the Edit icon.
3. In the Grid Member Properties editor, select the Network -> Advanced tab and complete the following:
   - Enable NAT Compatibility (IPv4 only): Select this check box. NAT group is not supported by IPv6 appliances.
   - NAT Group: From the drop-down list, select the NAT group you previously created.
   - NAT Addresses: For a single Grid Master or member, enter the address configured on the NAT appliance that maps to the interface address of the LAN1 port. A single master or member that serves DNS uses this NAT address for Grid communications and—if it serves DNS—DNS messages.

For an HA Grid Master or member, enter the address configured on the NAT appliance that maps to its VIP address. An HA master uses its VIP NAT address when communicating with Grid members. An HA member that serves DNS uses its VIP NAT address for its DNS messages. It uses its LAN1 port NAT address for Grid communications.

- **Node 1 (if HA)**
  - NAT IP Address: Enter the address configured on the NAT appliance that maps to the interface address of the LAN1 port on Node 1. When Node 1 of an HA member is active, it uses its NAT address for Grid communications.
- **Node 2 (if HA)**
  - NAT IP Address: Enter the address configured on the NAT appliance that maps to the interface address of the LAN1 port on Node 2. When Node 2 of an HA member is active, it uses its NAT address for Grid communications.

4. Save the configuration and click Restart if it appears at the top of the screen.

**Automatic Software Version Coordination**

When you add an appliance or HA pair to a Grid as a new member, it is important that it is running the same version of software as the other members in the Grid. Infoblox provides two methods for coordinating the software version:

- Manual Upgrade and Downgrade: Before adding an appliance or HA pair to a Grid, you can manually upgrade or downgrade the software on the appliance or HA pair to the version used by the rest of the Grid.
- Automatic Upgrade and Downgrade: The Grid Master automatically compares the software version of each appliance attempting to enter a Grid with that in use by the rest of Grid. If the versions do not match, the Grid Master downloads the correct version to the new appliance or HA pair.

**Note:** The Grid Master checks the software version every time an appliance or HA pair joins the Grid. The software version check occurs during the initial join operation and when a member goes offline and then rejoins the Grid.

*Figure 5.7 Automatic Upgrade of An Appliance Joining a Grid*
When a single appliance attempts to join the Grid for the first time, the following series of events takes place:

1. The appliance establishes an encrypted VPN tunnel with the Grid Master.
2. The master detects that the software version on the appliance is different from that in the rest of the Grid. For example, the appliance is running NIOS 6.10.0 software but the rest of the Grid is running NIOS 7.3.200 software.
3. The appliance downloads the NIOS 7.3.200 software from the Grid Master.
4. After the upgrade is complete, the NIOS application automatically restarts.
5. After the appliance reboots, it again contacts the Grid Master and step 1 is repeated. Because the software versions now match, the appliance can complete its attempt to join the Grid.

When an HA pair attempts to join the Grid for the first time, the following series of events takes place:

1. The active node of the HA pair establishes an encrypted VPN tunnel with the Grid Master.
2. The master detects that the software version on the node is different from that in the rest of the Grid. For example, the active node is running NIOS 6.10.0 software but the rest of the Grid is running NIOS 7.3.200 software.
3. The appliance downloads the NIOS 7.3.200 software from the Grid Master.
4. After the upgrade is complete, the NIOS application on the active node automatically restarts. This causes an HA failover.
5. The new active node (which was previously the passive node) attempts to join the Grid, repeating steps 1 – 4.
6. When the NIOS application on the currently active node restarts, there is another failover, and the currently passive node becomes active again.
7. The active node again contacts the Grid Master and step 1 is repeated. Because the software versions now match, it can complete its attempt to join the Grid.

**Grid Bandwidth Considerations**

Infoblox Grid technology relies upon database replication for its core functionality. When designing a Grid, it is important to consider the amount of traffic generated by this replication and the overall number of Grid members. Other communication between Grid members (such as log retrieval and monitoring functions) occurs as well. All of this traffic is securely communicated between the Grid Master and Grid members through encrypted VPN tunnels.

One component of the traffic through the tunnels is database replication traffic. There are three types to consider:

- **Complete database replication to a Master Candidate** — Occurs when a Master Candidate joins or rejoins a Grid. The Grid Master sends the complete database to a Master Candidate so that it has all the data it needs if it ever becomes promoted from member to master.
- **Partial database replication** — Occurs when an appliance or HA pair joins or rejoins the Grid as a regular member (which is not configured as a Master Candidate). The Grid Master sends it the section of the database that mainly applies just to the member.
- **Ongoing database updates** — Occurs as changes are made to the Grid configuration and data. The Grid Master sends all ongoing database updates to Master Candidates and individual member-specific updates to regular members.

If there are no or very few DNS dynamic updates, and no or very few DHCP lease offers and renewals issued, then this type of replication traffic is minimal.

If there are many DDNS (dynamic DNS) updates (many per second) and/or many DHCP lease offers and renewals (many per second), then the replication traffic is the largest component of the VPN traffic among Grid members.
**Note:** A Grid Master replicates data to single members and to the active node of HA members. The active node then replicates the data to the passive node in the HA pair.

At a minimum, there must be 256 Kbps (kilobits per second) bandwidth between the Grid Master and each member, with a maximum round-trip delay of 500 milliseconds. For ongoing database updates, the amount of data sent or received is 15 Kb for every DDNS update, and 10 Kb for every DHCP lease-offer/renew. The baseline amount for heartbeat and other maintenance traffic for each member is 2 Kbps. Measure the peak DNS and DHCP traffic you see in your network to determine the bandwidth needed between the Grid Master and its members for this activity. For example, you might decide to place your Grid members in the locations shown in *Figure 5.6*.

*Figure 5.8 Grid Deployment*

In this example, the Grid Master is optimally placed in the Data Center West. There are a total of seven members: the HA Grid Master, three HA members, and three single members. If all the members are Master Candidates, the Grid Master replicates all changes to the other six members. Assuming that the master receives 20 dynamic updates per minute and 40 DHCP lease renewals per minute, the calculation for Grid bandwidth is:

\[
\begin{align*}
20 \text{ DDNS updates/minute/60 secs} & = 0.333 \text{ DDNS updates/sec} \times 15 \text{ Kb} \times 6 \text{ members} = 30 \text{ Kbps} \\
40 \text{ DHCP leases/minute/60 secs} & = 0.666 \text{ DHCP leases/sec} \times 10 \text{ Kb} \times 6 \text{ members} = 40.2 \text{ Kbps} \\
2 \text{ Kbps of Grid maintenance traffic} \times 6 \text{ members} & = 12 \text{ Kbps} \\
\text{Total} & = 82.2 \text{ Kbps}
\end{align*}
\]

Another component is the upgrade process. See *Upgrading NIOS Software* for more information. Bandwidth requirements, database size, and update rate determine the maximum size of the Grid you can deploy. Based on the various factors discussed above, you can determine the amount of bandwidth your Grid needs. If your calculations exceed the available bandwidth, then you might need to modify your deployment strategy, perhaps by splitting one large Grid into two or more smaller ones.

**Note:** This calculation does not take into account existing traffic other than DNS and DHCP services, so factor and adjust accordingly.

For international networks, because of bandwidth and delay requirements, a geographical grouping of Grid members might be the best approach. For example, if you have a global presence, it may make the most sense to have a North American Grid, a South American Grid, a European Grid, and an Asia/Pacific Grid.

**About HA Pairs**

You can configure two appliances as an HA (high availability) pair to provide hardware redundancy for core network services and Infoblox Advanced DNS Protection. For more information, see *Infoblox Advanced DNS Protection*. An HA pair can be a Grid Master, a Grid Master...
candidate, a Grid member, or an independent appliance. The two nodes that form an HA pair—identified as Node 1 and Node 2—are in an active/passive configuration. The active node receives, processes, and responds to all service requests. The passive node constantly keeps its database synchronized with that of the active node, so it can take over services if a failover occurs. A failover is the reversal of the active/passive roles of each node; that is, when a failover occurs, the previously active node becomes passive and the previously passive node becomes active. You can configure an HA pair in either IPv4, IPv6, or in dual mode. An IPv4 HA pair uses IPv4 as the communication protocol between the two nodes and an IPv6 HA pair uses IPv6 as the communication protocol between the two nodes. But in a dual mode HA pair, you can select either IPv4 or IPv6 as the communication protocol between the two nodes. Note that when you add a dual mode HA member to a Grid, the communication protocol between the two nodes of an HA pair must the same as the Grid communication protocol.

**Note:** HA Grid Master and HA Grid Master candidate configurations are not supported when Threat Protection licenses are installed on the appliance.

When you configure an HA pair using the IB-4030 (Rev-1 or Rev-2) appliance for DNS cache acceleration, the passive node does not operate with a pre-loaded cache or hot cache during a failover; it builds up the DNS cache over time. For more information about HA and other limitations for the IB-4030 appliances, refer to the [Infoblox DNS Cache Acceleration Application Guide](https://infoblox.com/docs/infoblox/dns-cache-acceleration).

For Infoblox, only the active node in an HA pair handles DNS traffic. The passive node is in a standby mode ready to take over if a failover occurs.

The appliance uses the following components in the HA functionality:

- bloxSYNC: An Infoblox proprietary mechanism for secure, real-time synchronization of the database that maintains the data, system configuration, and protocol service configuration between the two nodes. With bloxSYNC, the nodes continuously synchronize changes of their configurations and states. When a failover occurs, the passive node can quickly take over services. For information, see [About HA Failover](https://infoblox.com/docs/infoblox/ha).
- VRRP (Virtual Router Redundancy Protocol): An industry-standard, MAC-level HA failover mechanism. VRRP utilizes the concept of an active and passive node that share a single VIP (virtual IP) address. When the active node that owns the VIP becomes unavailable, the passive node takes over the VIP and provides network core services. For information about VRRP, refer to [RFC3768, Virtual Router Redundancy Protocol (VRRP)](https://tools.ietf.org/html/rfc3768) and [VRRP Advertisements](https://infoblox.com/docs/infoblox/vrrp).

Using bloxSYNC and VRRP combined, if the active node fails or is taken offline for maintenance purposes, the passive node assumes the VIP and continues to respond to requests and services with minimal interruption. You can deploy an HA pair as a Grid Master, a Grid member, or an independent HA. To deploy an independent HA pair, see [Deploying an Independent HA Pair](https://infoblox.com/docs/infoblox/ha-independent). To deploy an HA Grid Master, see [Creating a Grid Master](https://infoblox.com/docs/infoblox/ha-gridmaster).

**Planning for an HA Pair**

To achieve high availability, the HA and LAN1 (or VLAN) ports on both the active and passive nodes are connected to switches on the same network or VLAN. Both nodes in an HA pair share a single VIP address and a virtual MAC address so they can appear as a single entity on the network. You can also assign IPv6 addresses for each of the active and passive nodes, in addition to the IPv6 VIP address.

**Tip:** Infoblox uses VRRP advertisements for the active and passive HA design. Therefore, all HA pairs must be located in the same location connected to the highly available switching infrastructure. Any other deployment is not supported without a written agreement with Infoblox. Contact Infoblox Technical Support for more information about other deployment support.

**Note:** You can enable ARP on the passive node of an HA pair and monitor its status externally. To enable ARP on the passive node of an HA pair, see [Enabling ARP on the Passive Node of an HA Pair](https://infoblox.com/docs/infoblox/arp).

As illustrated in Figure 5.9, the VIP and virtual MAC addresses link to the HA port on each node. Select five IP addresses on the same network before you configure an HA pair, as follows:

- VIP: For core network services and for management purposes when the MGMT port is disabled. Both nodes share the same VIP.
- Node 1 HA (active): Source IP for the VIP and VRRP advertisements
- Node 1 LAN1 (active): For management through SSHv2 and listens for VRRP advertisements from the HA port
- Node 2 HA (passive): Listens for VRRP advertisements
- Node 2 LAN1 (passive): Source IP for SSL VPN to the VIP of the active node and receives bloxSYNC from the VIP

*Figure 5.9 HA Pair*
When you deploy a vNIOS HA pair, ensure that the port connection allows for more than one MAC address per vNIC. For example, if you deploy a vNIOS HA pair in VMware vSphere, the port-profile to which the vNIOS HA and LAN ports connect should allow for more than one MAC address per vNIC. You can do this by changing the security settings of the port-group to accept “MAC address changes” and “Forged transmits,” as illustrated in Figure 5.10.

*Figure 5.10 Configuring port-profile in VMware vSphere*

---

**About HA Failover**

The appliance supports HA through bloxHA™, which provides a robust failover mechanism. As described in Planning for an HA Pair, both nodes in an HA pair share a single VIP address and a virtual MAC address. The node that is currently active is the one whose HA port owns the VIP address and virtual MAC address. When a failover occurs, these addresses shift from the HA port of the previous active node to the HA port of the new active node, as illustrated in Figure 5.11.

*Note:* For a vNIOS HA pair, you must configure both LAN1 and HA interfaces to operate. When there is a notification about failure in any one of the port, make sure that both of these ports are working. If one of the port is down and another port is still working, the HA pair believes its peer is active. But, there will be connectivity issues as one of the port is down. An HA failover occurs on vNIOS appliances only when both of these ports are down. For details about configuring these virtual NICs, refer to the Infoblox Installation Guide vNIOS for VMware.
Figure 5.11 VIP Address and Virtual MAC Address and HA Failover

The clients always make service requests to—and receive replies from—the VIP and virtual MAC address.

After an HA Failover

The clients still make service requests to—and receive replies from—the same VIP and virtual MAC address.

After an HA failover occurs, Node 2 becomes the active node. Because Node 2 is now active, it now owns the VIP address and virtual MAC address.
Enabling ARP on the Passive Node of an HA Pair

You can enable ARP (Address Resolution Protocol) on the passive node of an HA pair and monitor its status externally. For example, when the active node of an HA pair fails over to the passive node, you can ping the passive node from an external location and monitor its status. By default, ARP is disabled on the passive node of an HA pair. ARP settings on an HA member are preserved during a system restart or reboot, HA switch over, and upgrade. In addition, you do not need to restart the appliance when you modify ARP settings. When the active node becomes passive during an HA failover, ARP on an HA member inherits the settings configured in the database.

You can view detailed status for both nodes of an HA pair through the Detailed Status panel. To view the Detailed Status panel, from the Grid tab, select the Grid Manager tab -> Members tab -> Grid member check box -> Detailed Status icon in the horizontal navigation bar. In the Detailed Status panel, you can view ARP connectivity status for the passive node of an HA pair (Green = The passive HA node is connected to the local router; Yellow = The passive HA node fails to connect to the local router; Gray = ARP is disabled on the passive node of an HA pair). The passive HA node uses arping to test the ARP connectivity with the local router. If the local router is not configured, you may see false warnings even if the ARP connectivity is fine. In case of an ARP connectivity failure, the appliance sends an SNMP trap and an email notification, if configured. Note that the ARP setting is not preserved on a passive HA node when you reset the appliance using the CLI command reset all or reset the database using the CLI command reset db. To enable ARP on an HA passive node:

1. From the Grid tab, select the Grid Manager tab -> Members tab.
2. Select an HA member and click the Edit icon.
3. In the Grid Member Properties editor, select the Network tab -> Advanced tab and complete the following:
   - Enable ARP on HA Passive Node?: Select one of the following:
     - Disable (default): Select this to disable ARP on an HA passive node. This is selected by default.
     - Enable (not recommended): Select this to enable ARP on an HA passive node.

**WARNING:** Enabling ARP on the passive node of an HA interface might affect VRRP on the local network and could cause the firewall to send false alerts.

4. Save the configuration and click Restart if it appears at the top of the screen.

HA Failover on DNS Nameservers

When an HA failover occurs on NIOS, there is an approximate 4-5 second time interval in which the network is adjusted for the new active node and the new passive node. During this failover period, the active node becomes unresponsive. After the new active node comes up on the network, the DNS service loads all Response Policy Zone (RPZ) files if RPZ is configured. The larger the RPZ files, the longer it takes to load them, and the longer it takes the DNS service to start serving DNS. For example, on a TE-1425 with RPZs that contain 15 million resource records, it can take approximately one and a half minutes to start serving DNS.

If your nameserver uses Grid replication to keep internal zones up to date and is not configured to use RPZ, then the delay before the DNS service starts serving DNS is slightly longer than it is for the HA failover itself.

VRRP Advertisements

VRRP advertisements are periodic announcements of the availability of the HA node linked to the VIP. The two nodes in an HA pair include a VRID (virtual router ID) in all VRRP advertisements and use it to recognize VRRP advertisements intended for themselves. Only another appliance on the same subnet configured to use the same VRID responds to the announcements. The active node in an HA pair sends advertisements as multicast datagrams every second. It sends them from its HA port using the source IP address of the HA port (not from the VIP address) and the source MAC address 00:00:5e:00:01:vrrp_id. The last two hexadecimal numbers in the source MAC address indicate the VRID number for this HA pair. For example, if the VRID number is 143, then the source MAC address is 00:00:5e:00:01:8f (8f in hexadecimal notation = 143 in decimal notation).

The destination MAC and IP addresses for all VRRP advertisements are 00:00:5e:00:01:12 and 224.0.0.18 (00:00:5e:00:02:12 and FF02::12 for IPv6 only configurations). Because a VRRP advertisement is a multicast datagram that can only be sent within the immediate logical broadcast domain, the nodes in an HA pair must be in the same subnet together.

As illustrated in Figure 5.12, when you configure an HA pair, only the appliance configured to listen for VRRP advertisements with the same VRID number processes the datagrams, while all other appliances ignore them. The passive node in an Infoblox HA pair listens for these on its HA port and the active node listens on its LAN1 or LAN1 (VLAN) port. If the passive node does not receive three consecutive advertisements or if it receives an advertisement with the priority set to 0 (which occurs when you manually perform a forced failover or request the active node to restart, reboot, or shut down), it changes to the active state and assumes ownership of the VIP address and virtual MAC address.

If both nodes go offline, the one that comes online first becomes the active node. If they come online simultaneously, or if they enter a dual-active state—that is, a condition arises in which both appliances assume an active role and send VRRP advertisements, possibly because of network issues—then the appliance with the numerically higher VRID priority becomes the active node. The priority is based on system status and events.

If both nodes have the same priority, then the appliance whose HA port has a numerically higher IP address becomes the active node. For example, if the IP address of the HA port on Node 1 is 10.1.1.80 and the IP address of the HA port on Node 2 is 10.1.1.20, then Node 1 becomes the active node.

For more information about VRRP, see RFC 3768, Virtual Router Redundancy Protocol (VRRP).

Figure 5.12 VRRP Advertisements with a Unique VRID
Note: For a dual mode (IPv4 and IPv6) HA Master or HA member, you can set either IPv4 or IPv6 for VRRP advertisements.

Creating a Grid Master

To create a Grid, you first create a Grid Master and then add members. Although the Grid Master can be a single appliance (a “single master”), a more resilient design is to use an HA pair (an “HA master”) to provide hardware redundancy. For information about HA pairs, see About HA Pairs. The basic procedure for forming two appliances into an HA master is shown in Figure 5.13. You can create a Grid Master in either IPv4, IPv6, or dual mode (IPv4 and IPv6). An IPv4 Grid Master uses IPv4 as the Grid communication protocol, so it supports IPv4 and dual mode Grid members. An IPv6 Grid Master uses IPv6 as the Grid communication protocol, so it supports IPv6 and dual mode Grid members. A dual mode Grid Master supports IPv4, IPv6, and dual mode Grid members. You can set either IPv4 or IPv6 as the communication protocol. All Infoblox hardware platforms, except for appliances with a 50 GB disk, support configuration as a Grid Master or Grid Master candidate. For information about which vNIOS appliance supports configuration as a Grid Master, see Supported vNIOS Appliance Models and Specifications.

Figure 5.13 Initially Configuring a Pair of Appliances as a Grid Master
After the two nodes form an HA pair, Node 2 initiates a key exchange and creates an encrypted VPN tunnel with Node 1. The two nodes communicate between the VIP interface linked to the HA port on Node 1 and the LAN1 port on Node 2. The initialization of VPN communications between the two nodes is shown in Figure 5.14.

Figure 5.14 Establishing a VPN Tunnel for Grid Communications
After the nodes establish a VPN tunnel between themselves, Node 1 sends Node 2 its entire database (its configuration settings and service data). Because the configuration contains the VRID (virtual router ID) for the HA pair, Node 2 starts listening for VRRP advertisements containing that VRID number. Because Node 1 is already sending such advertisements, Node 2 receives one and assumes the passive role in the HA pair. After the initial transmission of its database, Node 1 continues to send Node 2 real-time database updates through the VPN tunnel.

Node 1 maintains the synchronization of the database throughout the Grid—which, at this point, has no other members—sends VRRP advertisements indicating its physical and network health, and—if configured to do so—provides network services. Node 2 maintains a state of readiness to assume mastership in the event of a failover. You can see the flow of HA- and Grid-related traffic from ports on the active node to ports on the passive node in Figure 5.15. This illustration also shows the ports that you can use for management traffic and network service.

Figure 5.15 Traffic and Ports that an HA Grid Master Uses

Note:
If you enable the MGMT port, you can only make an HTTPS connection to the IP address of the active node. If you try to connect to the IP address of the passive node, the appliance redirects your browser to the IP address of the active node.

SSHv2, however, behaves differently from HTTPS. If you enable the MGMT port and define its network settings for both nodes in the HA pair, you can make an SSHv2 connection to the IP addresses of the LAN1 and MGMT ports on both the active and passive node.
From the management system, you can manage the active node of the HA master by making an HTTPS connection to the VIP interface and using the GUI, and making an SSHv2 connection to the LAN1 port (and MGMT port, if enabled) and using the CLI. If you enable the MGMT port on an HA pair, you can make an HTTPS connection through the MGMT port on the active node, and you can make an SSHv2 connection through the LAN1 or MGMT port on the active and passive nodes.

**Note:** For information about enabling and using the MGMT port, the Infoblox GUI, and SSH, see *Using the MGMT Port, Logging in to the GUI*, and *Restricting GUI/API Access*.

**Port Numbers for Grid Communication**

If connectivity between Grid members must pass through a firewall, the firewall policies must allow the initial key exchange and subsequent VPN traffic to pass. The key exchange uses UDP with a source and destination port of 2114. VPN traffic uses UDP with a default source and destination port of 1194. The VPN port number is configurable.

To configure the VPN port number:

1. From the **Grid** tab, select the **Grid Manager** tab.
2. Expand the Toolbar and click **Grid Properties -> Edit**.
3. In the **General** tab of the **Grid Properties** editor, type a new port number in the **VPN Port** field.
4. Save the configuration.
5. When Grid Manager displays a warning indicating that a product restart is required, click **Yes** to continue. The product automatically restarts.

A member and master first perform a handshake to authenticate each other and exchange encryption keys. Then they build an encrypted VPN tunnel between themselves. The member typically initiates both of these connections. The master only initiates a key exchange if you manually promote a member to the role of master (see *Promoting a Master Candidate*). Figure 5.14 shows the typical connection exchange and default port usage not only between the two nodes forming an HA pair but also between a member and master when the member joins a Grid. The member and master key exchange occurs when an appliance joins a Grid, during master promotion, and when a member reconnects to a Grid after becoming disconnected. At all other times, Grid-related communications occur through encrypted VPN tunnels.

**Grid Setup Wizard**

The Grid Setup Wizard simplifies configuring a Grid. You can use it to configure an HA or single Grid Master and to join appliances to a Grid. The Grid Setup Wizard appears when you first log in to the appliance. After that, you can access it at anytime as follows:

1. From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab.
2. Expand the Toolbar and click **Grid Properties -> Setup (Grid Setup Wizard)**.

**Creating an HA Grid Master**

To create a Grid, you first create a Grid Master and then add members. Although you can define a single appliance as a Grid Master, using an HA pair provides hardware redundancy for this vital component of a Grid. You can create an HA Master in either IPv4, IPv6, or in dual mode. An IPv4 HA Master uses IPv4 as the communication protocol between the two nodes and for Grid communication. An IPv6 HA pair uses IPv6 as the communication protocol between the two nodes and for Grid communication. But in a dual mode HA pair, you can select either IPv4 or IPv6 as the communication protocol between the two nodes and for Grid communication. The following procedure explains how to put two NIOS appliances on the network and use the Grid Setup Wizard to configure them as Nodes 1 and 2 to form an HA Grid Master. For information about which vNIOS appliance supports configuration as an HA Grid Master, see *Supported vNIOS Appliance Models and Specifications*.

**Configuring the Connecting Switch**

To ensure that VRRP (Virtual Router Redundancy Protocol) works properly, configure the following settings at the port level for all the connecting switch ports (HA, LAN1, and LAN2):

- Spanning Tree Protocol: Disable this or enable this with Portfast. For vendor specific information, search for “HA” in the Infoblox Knowledge Base system at [https://support.infoblox.com](https://support.infoblox.com).
- Trunking: Disable
- EtherChannel: Disable
- IGMP Snooping: Disable
- DHCP Snooping: Disable or Enable Trust Interface

**Note:** You must disable DHCP Snooping to successfully run DHCP services on the Grid. For more information about DHCP services, see *About Infoblox DHCP Services*.

- Port Channeling: Disable
- Speed and Duplex settings: Match these settings on both the Infoblox appliance and switch
- Disable other dynamic and proprietary protocols that might interrupt the forwarding of packets

**Note:** By default, a NIOS appliance automatically negotiates the optimal connection speed and transmission type (full or half duplex) on the physical links between its LAN1 or LAN1 (VLAN), HA, and MGMT ports and the Ethernet ports on the connecting switch. If the two appliances fail...
Placing Both Appliances on the Network

1. Connect the power cable from each NIOS appliance to a power source and turn on the power. If possible, connect the appliances to separate power circuits. If one power circuit fails, the other might still be operative.

2. Connect Ethernet cables from the LAN1 port and the HA port on each appliance to a switch on the network.

Note: The Ethernet ports on the TE-810, TE-820, TE-1410, TE-1420, TE-2210, TE-2220, and IB-4010 appliances are autosensing, so you can use either a straight-through or cross-over Ethernet cable for these connections.

3. Use the LCD on one appliance or make a console connection to it, and configure the network settings of its LAN1 port so that it is on the local subnet and you can reach it on the network. LCD supports only IPv4 addressing and not IPv6 addressing. You can configure IPv6 address for the appliance through CLI or GUI. IPv4 addressing is supported on the LCD: ensure that you have the correct network address values before configuration of the appliance.

Note: For details about using the LCD and console, refer to the installation guide that shipped with your product.

4. Similarly, configure the LAN1 port on the other appliance so that it is in the same subnet as the first appliance.

5. Connect your management system to the network so that it can reach the IP addresses of the LAN1 ports on both appliances.

HA Master – Node 1

1. On your management system, open a browser window, and connect to https://ip_addr, where ip_addr is the address of the LAN1 port on Node 1. IPv4 and IPv6 values are valid, based on the LAN1 port configuration.

2. Log in using the default user name and password admin and infoblox. For detailed information about logging in to the GUI, see Logging in to the GUI.

3. Review the End-User License Agreement. If you want to participate in the Infoblox Customer Experience Improvement Program, complete the following:

- **Participate in the Infoblox Customer Experience Improvement Program**: Select the check box to send product usage data to Infoblox on a periodic basis. Infoblox uses this data to improve product functionality. For more information about the program, see Participating in the Customer Experience Improvement Program.

- **Support ID (optional)**: Enter the Infoblox Support ID that was assigned to your account. It must be a number with four to six digits. The value you enter here is also displayed in the Customer Improvement tab in the Grid Properties editor. Infoblox includes this ID in the data report.

- **Infoblox Privacy Policy**: Click here to view the Infoblox privacy policy. The appliance displays the policy in a new browser tab.

Click I Accept. The Grid Setup wizard appears.

4. On the first screen, select Configure a Grid Master and click Next.

5. On the next screen, specify the Grid properties and click Next:

- **Grid Name**: Enter a text string that the two appliances use to authenticate each other when establishing a VPN tunnel between them. The default Grid name is Infoblox.

- **Shared Secret**: Enter a text string that both appliances use as a shared secret to authenticate each other when establishing a VPN tunnel between them. The default shared secret is test.

- **Confirm Shared Secret**: Enter the shared secret again.

- **Hostname**: Enter a valid domain name for the appliance.
  - **Type of Network Connectivity**: Select the type of network connectivity from the drop-down list:
    - IPv4 and IPv6: Select this to configure a dual mode HA Master.
    - IPv4: Select this to configure an IPv4 HA Master.
    - IPv6: Select this to configure an IPv6 HA Master.

- **Is the Grid Master an HA pair?**: Select Yes.
  - **Send HA and Grid Communication over**: This field is displayed only when you are configuring a dual mode HA pair. Select either IPv4 or IPv6 as the communication protocol for VRRP advertisements.

Note: Infoblox recommends that you backup the configuration after you convert a Grid to a different mode. Restoring the old backup by performing a forced restore, may prevent the Grid members from rejoining the Grid Master after the restore.

6. On the next screen, specify the network properties and click Next:

- **Virtual Router ID**: Enter the VRID (virtual router ID). This must be a unique VRID number—from 1 to 255—for this subnet.

- **Ports and Addresses**: This table lists the network interfaces based on the type of network connectivity of the HA Master.
  - For IPv4 HA Master, specify the network information for VIP (IPv4), Node1 HA (IPv4), Node2 HA (IPv4), Node1 LAN1 (IPv4), and Node2 LAN1 (IPv4) interfaces.
  - For IPv6 HA Master, specify the network information for VIP (IPv6), Node1 LAN1 (IPv6), and Node2 LAN1 (IPv6) interfaces.

For a dual mode HA Master, if you select IPv4 in the Send HA and Grid Communication over field, specify the network information for the following interfaces: VIP (IPv4), Node1 HA (IPv4), Node1 LAN1 (IPv4), Node2 HA (IPv4), Node2 LAN1 (IPv4), VIP (IPv4), VIP (IPv6), Node1 LAN1 (IPv6), and Node2 LAN1 (IPv6) interfaces.

For a dual mode HA Master, if you select IPv6 in the Send HA and Grid Communication over field, specify the network information for the following interfaces: VIP (IPv4), Node1 LAN1 (IPv4), Node2 LAN1 (IPv4), VIP (IPv6), Node1 LAN1 (IPv6), and Node2 LAN1 (IPv6) interfaces.
interfaces.

Enter correct information for the following by clicking the field:

- **Interface**: Displays the name of the interface. You cannot modify this.
- **Address**: Type the IPv4 or IPv6 address depending on the type of interface.
- **Subnet Mask (IPv4) or Prefix Length (IPv6)**: Specify an appropriate subnet mask for IPv4 address or prefix length for IPv6 address. The prefix length ranges from 2 to 127.
- **Gateway**: Type the IPv4 or IPv6 address of the default gateway depending on the type of interface. For IPv6 interface, you can also type **Automatic** to enable the appliance to acquire the IPv6 address of the default gateway and the link MTU from router advertisements.

**Note**: You can now define a link-local address as the default IPv6 gateway and isolate the LAN segment so the local router can provide global addressing and access to the network and Internet. This is supported for both LAN1 and LAN2 interfaces as well as LAN1 and LAN2 in the failover mode.

- **VLAN Tag**: For a VLAN, enter the VLAN tag or ID. You can enter a number from 1 to 4094. Ensure that you configure the corresponding switch accordingly.
- **Port Settings**: From the drop-down list, choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose **Full** for concurrent bidirectional data transmission or **Half** for data transmission in one direction at a time. Select **Automatic** to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOS appliances.

7. Optionally, enter a new password and click **Next**. The password must be a single string (no spaces) that is at least four characters long.

8. Select the time zone of the Grid Master and indicate whether the Grid Master synchronizes its time with an NTP (Network Time Protocol) server.
   - If you choose to enable NTP, click the Add icon and enter the IP address of an NTP server. Entries may be an IPv4 or IPv6 address. You can enter IP addresses for multiple NTP servers.
   - If you choose to disable NTP, set the date and time for the appliance.
   - Click **Next**.

9. If you want to participate in the Infoblox Customer Experience Improvement Program, complete the following and then click **Next**:
   - **Participate in the Infoblox Customer Experience Improvement Program**: Select the check box to send product usage data to Infoblox on a periodic basis. Infoblox uses this data to improve product functionality. For more information about the program, see **Participating in the Customer Experience Improvement Program**.
   - **Support ID (optional)**: Enter the Infoblox Support ID that was assigned to your account. It must be a number with four to six digits. The value you enter here is also displayed in the **Customer Improvement** tab in the Grid Properties editor. Infoblox includes this ID in the data report.
   - **Email**: Enter an email address to which Infoblox sends a copy of the usage report. The email address you enter here is also displayed in the **Customer Improvement** tab in the Grid Properties editor. This is optional.
   - **Infoblox Privacy Policy**: Click here to view the Infoblox privacy policy. The appliance displays the policy in a new browser tab.

10. The last screen displays the settings you specified in the previous panels of the wizard. Verify that the information is correct and click **Finish**. The application restarts after you click **Finish**.

**Note**: The Grid Setup wizard provides options such as not changing the default password and manually entering the time and date. However, changing the password and using an NTP server improve security and accuracy (respectively), and so these choices are presented here. Record and retain this information in a safe place. If you forget the shared secret, you need to contact Infoblox Technical Support for help. When you add an appliance to the Grid, you must configure it with the same Grid name, shared secret, and VPN port number that you configure on the Grid Master.

11. Close the management window.

The configuration for Node 1 is complete.

**HA Master – Node 2**

1. On your management system, open a new browser window, and connect to https://ip_addr, where ip_addr is the address of the LAN1 port on Node 2. IPv4 or IPv6 values are valid. When you enter an IPv6 address, enclose the address in square brackets (as in https://[ip_addr] or https://[2001:db8::256:ABCD:EF12:34:1]).
2. Log in using the default user name and password admin and infoblox.
3. Review the End-User License Agreement. If you want to participate in the Infoblox Customer Experience Improvement Program, complete the following:
   - **Participate in the Infoblox Customer Experience Improvement Program**: Select the check box to send product usage data to Infoblox on a periodic basis. Infoblox uses this data to improve product functionality. For more information about the program, see **Participating in the Customer Experience Improvement Program**.
   - **Support ID (optional)**: Enter the Infoblox Support ID that was assigned to your account. It must be a number with four to six digits. The value you enter here is also displayed in the **Customer Improvement** tab in the Grid Properties editor. Infoblox includes this ID in the data report.
- **Infoblox Privacy Policy**: Click here to view the Infoblox privacy policy. The appliance displays the policy in a new browser tab.

Click I Accept. The Grid Setup wizard appears.

4. On the first screen, select **Join Existing Grid** and click Next.

5. On the next screen, specify the Grid properties and click Next.

   - **Grid Name**: Enter a text string that the two appliances use to authenticate each other when establishing a VPN tunnel between them. This must match the Grid name you entered for node 1.
   - **Grid Master’s IP Address**: Enter the same VIP you entered for node 1.
   - **Shared Secret**: Enter a text string that both appliances use as a shared secret to authenticate each other when establishing a VPN tunnel between them. This must match your entry in node 1.

6. On the next screen verify the IP address settings of the member and click Next. The last screen displays the settings you specified in the previous panels of the wizard.

7. Verify that the information is correct and click Finish. The setup of the HA master is complete. From now on, when you make an HTTPS connection to the HA pair, use the VIP address. The communication protocol for all the services in a dual mode (IPv4 and IPv6) HA Master is the same protocol as the one used for VRRP advertisements. For example, if you select **IPv4** in the **Send HA and Grid Communication over** field in step 2 of the Grid Setup wizard, then IPv4 is set as the communication protocol for all the services. However, you can override the communication protocol for all the services in a dual mode HA Master. For information, see Changing the Communication Protocol for a Dual Mode Appliance.

### Creating a Single Grid Master

Although using an HA master is ideal because of the hardware redundancy it provides, you can also use a single appliance as the Grid Master. You can create a single Grid Master in either IPv4, IPv6, or dual mode (IPv4 and IPv6). Infoblox recommends frequent backups if the Grid Master is a single appliance, and there is no Master Candidate. For information about which vNIOS appliance supports configuration as a single Grid Master, see Supported vNIOS Appliance Models and Specifications.

Setting up an appliance as a single Grid Master is very easy. If the appliance has the DNSone package with the Grid upgrade, it is already a Grid Master. You simply need to define the network settings for its LAN1 port. The various procedures for defining the network settings for the LAN1 port of a single independent appliance apply here as well; that is, you can use any of the following procedures to define the network settings for the LAN1 port of the appliance that you want to make a single Grid Master:

- **LCD** – See Method 1 – Using the LCD. (LCD configuration does not support IPv6 address entry.)
- **Console port** – Method 2 – Using the CLI/4.

You can also use the NIOS Grid Setup Wizard to create a single Grid Master. In addition to providing a simple method accompanied by helpful information, the setup wizard allows you to change the admin password and configure time settings for the appliance.

### Using the Setup Wizard

To create a single Grid Master using the Grid Setup wizard:

1. Connect the power cable from the NIOS appliance to a power source and turn on the power.

2. Connect an Ethernet cable from the LAN1 port on the appliance to a switch on the network.

**Note**: The Ethernet ports on the TE-810, TE-820, TE-1410, TE-1420, TE-2210, TE-2220, and IB-4010 appliances are autosensing, so you can use either a straight-through or cross-over Ethernet cable for these connections.

3. If you have not changed the default IP address (192.168.1.2/24) of the LAN1 port through the LCD or CLI—and the subnet to which you connect the appliance does not happen to be 192.168.1.0/24—put your management system in the 192.168.1.0/24 subnet and connect an Ethernet cable between your management system and the NIOS appliance.

4. Open a web browser and make an HTTPS connection to the IP address of the LAN1 port. To reach the default IP address, enter: "https://192.168.1.2".

   Several certificate warnings appear during the login process. This is normal because the preloaded certificate is self-signed (and, therefore, is not in the trusted certificate stores in your browser) and has the hostname [www.infoblox.com](http://www.infoblox.com), which does not match the destination IP address you entered in step 3. To stop the warning messages from occurring each time you log in to the GUI, you can generate a new self-signed certificate or import a third-party certificate with a common name that matches the FQDN (fully qualified domain name) of the appliance. For information about certificates, see Managing Certificates.

5. Log in using the default user name admin and password infoblox.

6. Review the End-User License Agreement. If you want to participate in the Infoblox Customer Experience Improvement Program, complete the following:

   - **Participate in the Infoblox Customer Experience Improvement Program**: Select the check box to send product usage data to Infoblox on a periodic basis. Infoblox uses this data to improve product functionality. For more information about the program, see Participating in the Customer Experience Improvement Program.
   - **Support ID (optional)**: Enter the Infoblox Support ID that was assigned to your account. It must be a number with four to six digits. The value you enter here is also displayed in the Customer Improvement tab in the GridProperties editor. Infoblox includes this ID in the data report.
Click I Accept. The Grid Setup wizard appears.

7. On the first screen, select Configure a Grid Master and click Next.
8. On the next screen, specify the Grid properties and click Next:
   - Grid Name: Enter a text string that the Grid Master and appliances joining the Grid use to authenticate each other when establishing a VPN tunnel between them. The default Grid name is Infoblox.
   - Shared Secret: Enter a text string that the Grid Master and appliances joining the Grid use as a shared secret to authenticate each other when establishing a VPN tunnel between them. The default shared secret is test.
   - Confirm Shared Secret: Enter the shared secret again.
   - Hostname: Enter a valid domain name for the appliance.
   - Type of Network Connectivity: Select the type of network connectivity for the Grid Master from the drop-down list:
     - IPv4 and IPv6: Select this to configure a dual mode Grid Master.
     - IPv4: Select this to configure an IPv4-only Grid Master.
     - IPv6: Select this to configure an IPv6-only Grid Master.

Note: Infoblox recommends that you backup the configuration after you convert a Grid to a different mode. Restoring the old backup by performing a forced restore, may prevent the Grid members from rejoining the Grid Master after the restore.

9. On the next screen, configure the network settings and click Next:
   - Ports and Addresses: This table lists the network interfaces based on the type of network connectivity of the Grid Master. For IPv4 Grid Master, specify the network information for LAN1 (IPv4) port and for IPv6 Grid Master, specify the network information for LAN1 (IPv6) port. For a dual mode Grid Master, specify the network information for both LAN1 (IPv4) and LAN1 (IPv6).
     - Interface: Displays the name of the interface. You cannot modify this.
     - Address: Type the IPv4 or IPv6 address depending on the type of interface. An IPv6 address is a 128-bit number in colon hexadecimal notation. It consists of eight 16-bit groups of hexadecimal digits separated by colons (example: 2001:db8:0000:0123:4567:89ab:0000:00df or 2001:db8::123:4567:89ab:0000:00df).
     - Subnet Mask (IPv4) or Prefix Length (IPv6): Specify an appropriate subnet mask for IPv4 address or prefix length for IPv6 address. The prefix length ranges from 2 to 127.
     - Gateway: Type the IPv4 or IPv6 address of the default gateway depending on the type of interface. For IPv6 interface, you can also type Automatic to enable the appliance to acquire the IPv6 address of the default gateway and the link MTU from router advertisements.

   Note: You can now define a link-local address as the default IPv6 gateway and isolate the LAN segment so the local router can provide global addressing and access to the network and Internet. This is supported for both LAN1 and LAN2 interfaces as well as LAN1 and LAN2 in the failover mode.

9. On the next screen, configure the network settings and click Next:
   - VLAN Tag: For a VLAN, enter the VLAN tag or ID. You can enter a number from 1 to 4094. Ensure that you configure the corresponding switch accordingly.
   - Port Settings: From the drop-down list, choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose Full for concurrent bidirectional data transmission or Half for data transmission in one direction at a time. Select Automatic to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOS appliances.

10. Optionally, enter a new password and click Next. The password must be a single hexadecimal string (no spaces) that is at least four characters long.
11. Select the time zone of the Grid Master and indicate whether the Grid Master synchronizes its time with an NTP (Network Time Protocol) server, and then click Next:
   - If you choose to enable NTP, click the Add icon and enter the IP address of an NTP server. Entries may be an IPv4 or IPv6 address. You can enter IP addresses for multiple NTP servers.
   - If you choose to disable NTP, set the date and time for the appliance.

12. If you want to participate in the Infoblox Customer Experience Improvement Program, complete the following and then click Next:
   - Participate in the Infoblox Customer Experience Improvement Program: Select the check box to send product usage data to Infoblox on a periodic basis. Infoblox uses this data to improve product functionality. For more information about the program, see Participating in the Customer Experience Improvement Program.
   - Support ID (optional): Enter the Infoblox Support ID that was assigned to your account. It must be a number with four to six digits. The value you enter here is also displayed in the Customer Improvement tab in the GridProperties editor. Infoblox includes this ID in the data report.
   - Email: Enter an email address to which Infoblox sends a copy of the usage report. The email address you enter here is also displayed in the Customer Improvement tab in the Grid Properties editor. This is optional.
   - Infoblox Privacy Policy: Click here to view the Infoblox privacy policy. The appliance displays the policy in a new browser tab.

13. The last screen displays the settings you specified in the previous panels of the wizard. Verify that the information is correct and click Finish.
The application restarts after you click **Finish**.

**Note:** The Grid Setup wizard provides options such as not changing the default password and manually entering the time and date. However, changing the password and using an NTP server improve security and accuracy (respectively), and so these choices are presented here. Record and retain this information in a safe place. If you forget the shared secret, you need to contact Infoblox Technical Support for help. When you add an appliance to the Grid, you must configure it with the same Grid name, shared secret, and VPN port number that you configure on the Grid Master.

The last screen of the setup wizard states that the changed settings require the appliance to restart. When you click **Finish**, the appliance restarts.

The setup of the single master is complete. From now on, when you make an HTTPS connection to the appliance, use its new IP address.

In a dual mode Grid Master, the communication protocol for all the services is set to IPv4, by default. You can change the default communication protocol for the services. For information, see *Changing the Communication Protocol for a Dual Mode Appliance*.

### Adding Grid Members

**Note:** You may provision a Port Reservation for the new Grid Member. When doing so, you select the device to which you expect the new Grid Member to connect; In the context of a Grid member, this device type is usually an Ethernet Switch or Switch-Router. The Add Grid Member Wizard provides a step in which you define the port reservation settings, as described in the following section *Adding a Single Member*. The process also can be applied when defining an HA pair, as described in the sections *Creating an HA Grid Master* and *Adding an HA Member*.

You can add single appliances and HA pairs to a Grid, forming single members and HA members respectively. A single Grid member can be either an Infoblox appliance or a vNIOS appliance. You can configure Grid members in either IPv4, IPv6, or dual mode (IPv4 and IPv6). For information about which vNIOS appliance supports configuration as an HA Grid member, see *Supported vNIOS Appliance Models and Specifications*. You can also define an HA member on the Grid Master and then add two individual NIOS appliances to the Grid as Node 1 and Node 2 to complete the HA member you defined on the master.

New members inherit all settings that you create at the Grid level unless you override them at the member level. You can also define port reservations for the network infrastructure devices to which the Grid members will connect.

The process for adding either a single appliance or HA pair to a Grid involves the following steps:

1. Adding and configuring Grid members on the Grid Master. In addition to defining the network and appliance settings for a member, you can also configure service settings before you join the member or HA pair to the Grid.
2. Reserving a port on a switch or switch-router for connectivity to the Grid member.
3. Joining the appliance or HA pair to the Grid. This includes defining the VIP or IP address of the Grid Master, the Grid name, and the shared secret on the single appliance or HA pair. If an appliance or HA pair cannot join the Grid because of MTU (maximum transmission unit) limitations on its network link, you can reduce the MTU that the master uses when communicating with it. See *Setting the MTU for VPN Tunnels*. If the Grid Master is behind a NAT device and there are members on both sides of that NAT device, you must create a NAT group, as described in *NAT Groups*.

In a large scale deployment of Grids across multiple sites, consider remotely provisioning your Grid members before joining them to the Grid. For more information about this feature, see *Auto-Provisioning NIOS Appliances*.

In situations where you want to define certain configurations on an offline Grid member and associate DNS and DHCP data to the member before deploying it, you can use the pre-provisioning feature to accomplish this. For more information, see *Pre-Provisioning NIOS and vNIOS Appliances*.

### Adding a Single Member

The basic steps necessary to add a single member are as follows:

1. Define the network settings of the LAN1 port of the single appliance on the Grid Master.
2. Initiate the join Grid operation during which you specify the VIP or IP address of the Grid Master, the Grid name, and the shared secret on the single appliance. For information, see *Joining Appliances to the Grid*.

On the Grid Master, you can configure any service settings such as DNS zones and records, DHCP networks and address ranges, and other services for a member before or after you join the appliance to the Grid. The basic steps for adding a single member are presented in the following section.

For information on how to configure a vNIOS appliance as a Grid member, refer to the *Quick Start Guide for Installing vNIOS Software on Riverbed Services Platforms* and the *Quick Start Guide for Installing vNIOS Software on VMware Platforms*.

### Configuring a Single Member on the Grid Master

1. From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab.
2. Expand the Toolbar and click **Add** -> **Add Grid Member**.
3. In the **Add Grid Member** wizard, enter the following and click **Next**:
   - **Member Type:** Specify the appliance type of the Grid member. If the member is an Infoblox appliance, select **Infoblox**, which is the default. For a vNIOS appliance, select **Riverbed**, or **Virtual NIOS** for vNIOS virtual appliances, including cloud virtual appliances.
   - **Host Name:** Type the FQDN (fully qualified domain name) of the appliance that you are adding to the Grid.

Copyright ©2019, Infoblox, Inc. All right reserved.
4. Enter the following information about the member that you are adding to the Grid and click Next:

- **Type of Network Connectivity**: Select the type of network connectivity for the Grid member from the drop-down list:
  - IPv4 and IPv6: Select this to configure a dual mode Grid member.
  - IPv4: Select this to configure an IPv4 Grid member.
  - IPv6: Select this to configure an IPv6 Grid member.

**Note**: Infoblox recommends that you backup the configuration after you convert a Grid to a different mode. Restoring the old backup by performing a forced restore, may prevent the Grid members from rejoining the Grid Master after the restore.

- **Standalone Member**: Select this option.
- **Required Ports and Addresses**: This table lists the network interfaces based on the type of network connectivity of the Grid member. For IPv4 Grid member, specify the network information for LAN1 (IPv4) port and for IPv6 Grid member, specify the network information for LAN1 (IPv6) port. For a dual mode Grid member, specify the network information for both LAN1 (IPv4), and LAN1 (IPv6).

Enter correct information for the following by clicking the field:

- **Interface**: Displays the name of the interface. You cannot modify this.
- **Address**: Type the IPv4 or IPv6 address depending on the type of interface. An IPv6 address is a 128-bit number in colon hexadecimal notation. It consists of eight 16-bit groups of hexadecimal digits separated by colons (example: 2001:db8:0000:123:4567:89ab:0000:cdef or 2001:db8::123:4567:89ab:0.cdef).
- **Subnet Mask (IPv4) or Prefix Length (IPv6)**: Specify an appropriate subnet mask for IPv4 address or prefix length for IPv6 address. The prefix length ranges from 2 to 127.
- **Gateway**: Type the IPv4 or IPv6 address of the default gateway depending on the type of interface. For IPv6 interface, you can also type Automatic to enable the appliance to acquire the IPv6 address of the default gateway and the link MTU from router advertisements.
- **VLAN Tag (IPv4)** or **VLAN ID (IPv6)**: For a VLAN, enter the VLAN tag or ID. You can enter a number from 1 to 4094. Ensure that you configure the corresponding switch accordingly.
- **Port Settings**: From the drop-down list, choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose Full for concurrent bidirectional data transmission or Half for data transmission in one direction at a time. Select Automatic to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOS appliances.
- **DSCP Value**: Displays the Grid DSCP value, if configured. To modify, click Override and enter the DSCP value. You can enter a value from 0 to 63. For information about DSCP, see *Implementing Quality of Service Using DSCP*.

5. In the Port Reservation page, do the following:

Begin by checking the Reserve Port check box. Note that reserving a switch port does not guarantee its availability once the device must connect. The port is automatically assigned for connectivity to the LAN1 port on the appliance.

Optionally, you can skip connecting port configuration by clicking Next. Click the Clear button to remove the selected device from the configuration.

- **Click** the Select Device button to choose the device for which the port reservation will be associated. You should know the identity of the device to which the Infoblox appliance will connect before taking this step. For Grid member connectivity, the chosen device should be either a switch or a switch-router.
- **After** choosing the device, choose the **Interface** with which the reservation will be bound. The drop-down list shows only interfaces that are most recently found to be available by Grid Manager during the last Discovery cycle. This list will not include any ports that are Administratively Up and Operationally Up or that are otherwise already assigned to other networks or Objects.
- **The Wizard page also shows a list of any VLANs that are currently configured in the chosen device (The following VLANs are configured).** This Wizard page does not allow the definition of new VLANs for port configuration—only the assignment of an existing VLAN in the device to your new port reservation. (Recall that you may specify the **VLAN Tag** across which Grid member traffic will travel, when you specified the Grid member information in Step 2 of the Wizard.)
- **Check** the Configure Port check box to enter Port Control settings for the port reservation.
- **Choose** the Data VLAN and/or the Voice VLAN settings you may need for the port assignment. Depending on the selected device, the Voice VLAN field may or may not appear.
- **Set** the Admin Status to Up if you need to activate the port after assignment in the current task.
  - All **Port Control operations** require CLI credentials to be entered into Grid Manager. Because some IPAM and DHCP Objects will use Port Control features as part of object creation, CLI credentials are automatically leveraged as part of discovery. Ensure you have the correct sets of CLI credentials for devices in your network.
- **Enter** a Description for the port assignment. Infoblox recommends doing so to help other technicians to recognize the port assignment event.
- When finished, click Next to continue in the wizard.

6. Optionally, define extensible attributes. For information, see *About Extensible Attributes*.

7. The final step for adding a Grid member is to define when the associated Port Configuration task executes. You may execute it immediately or schedule it for another time and date.

- **To create** the new port configuration immediately, select Now. The port control task is automatically synchronized to take place at the
same time as the activation of the new Grid member.

- You can choose to have Grid Manager execute the port control task at a later time. To do so, select Later. Choose a Selected time by entering or selecting a Start Date (click the calendar icon to choose a calendar date) and a Start Time, and choose a Time Zone.

8. Choose one of the following from the Save &... drop-down button menu:
   - Click Save & Close to add the single member to the Grid and close the wizard (this is the default).
   - Click Save & Edit to add the single member to the Grid and launch the editor. You can configure additional properties, such as the MTU size, or add the member to a NAT group.
   - Click Save & New to add the single member to the Grid and launch the wizard again to add another member.

The communication protocol for all the services in a dual mode (IPv4 and IPv6) Grid member is set to IPv4, by default. You can change the default communication protocol for all the services. For information, see Changing the Communication Protocol for a Dual Mode Appliance.

Adding an HA Member

The basic steps necessary to add an HA member are as follows:

1. Define the network settings of the HA pair on the Grid Master.
2. Initiate the join Grid operation, during which you specify the VIP or IP address of the Grid Master, the Grid name, and the shared secret on the HA pair. For information, see Joining Appliances to the Grid.

In addition, on the Grid Master you can configure the service settings such as DNS zones and records, DHCP networks and address ranges, and so on for a member before or after you join the HA pair to the Grid. The basic steps for adding an HA member are presented below.

**Note:** The procedure for adding an HA pair to a Grid when it uses the MGMT port of the active node for Grid communications differs slightly from that described below. See Grid Communications.

Configuring an HA Member on the Grid Master

1. From the Grid tab, select the Grid Manager tab -> Members tab.
2. Expand the Toolbar and click Add -> Add Grid Member.
3. In the Add Grid Member wizard, enter the following and click Next:
   - **Member Type:** Specify the appliance type of the Grid member. If the member is an Infoblox appliance, select Infoblox, which is the default. For a vNIOS appliance on VMware, select Virtual NIOS.
   - **Host Name:** Type the FQDN (fully qualified domain name) for the HA member.
   - **Time Zone:** If you want the Grid member to have a different time zone, click Override and select a time zone.
   - **Comment:** Type a comment that provides some useful information about the appliance, such as its location.
   - **Master Candidate:** select this check box to designate this appliance as a Master Candidate. For supported vNIOS appliances, see Supported vNIOS Appliance Models and Specifications.
4. Enter the following information about the member that you are adding to the Grid and click Next:
   - **Type of Network Connectivity:** Select the type of network connectivity for the HA member from the drop-down list:
     - IPv4 and IPv6: Select this to configure a dual mode HA member.
     - IPv4: Select this to configure an IPv4 HA member.
     - IPv6: Select this to configure an IPv6 HA member.
   - **High Availability Pair:** Select this option.
   - **Virtual Router ID:** Enter a unique VRID number—from 1 to 255—for the local subnet.
   - **Send HA and Grid Communication Over:** This field is displayed only when you are configuring a dual mode HA member. Select either IPv4 or IPv6 as the communication protocol for VRRP advertisements and for joining the Grid Master.

**Note:** Infoblox recommends that you backup the configuration after you convert a Grid to a different mode.

Restoring the old backup by performing a forced restore, may prevent the Grid members from rejoining the Grid Master after the restore.

- **Required Ports and Addresses:** This table lists the network interfaces based on the type of network connectivity. For IPv4 HA member, specify the network information for VIP (IPv4), Node1 HA (IPv4), Node2 HA (IPv4), Node1 LAN1 (IPv4), and Node2 LAN1 (IPv4) interfaces. For IPv6 HA member, specify the network information for VIP (IPv6), Node1 LAN1 (IPv6), and Node2 LAN1 (IPv6) interfaces. For a dual mode HA member, if you select IPv4 in the Send HA and Grid Communication over field, specify the network information for the following interfaces: VIP (IPv4), Node1 HA (IPv4), Node1 LAN1 (IPv4), Node2 HA (IPv4), Node2 LAN1 (IPv4), VIP (IPv4), Node1 LAN1 (IPv6), and Node2 LAN1 (IPv6) interfaces. For a dual mode HA member, if you select IPv6 in the Send HA and Grid Communication over field, specify the network information for the following interfaces: VIP (IPv6), Node1 LAN1 (IPv6), Node2 LAN1 (IPv6), VIP (IPv6), Node1 LAN1 (IPv6), and Node2 LAN1 (IPv6) ports.

Enter correct information for the following by clicking the field:

- **Interface:** Displays the name of the interface. You cannot modify this.
- **Address:** Type the IPv4 or IPv6 address depending on the type of interface. An IPv6 address is a 128-bit number in colon hexadecimal notation. It consists of eight 16-bit groups of hexadecimal digits separated by colons (example: 2001:db8:0000:0123:4567:89ab:0000:cdef or 2001:db8::123:4567:89ab:0:cdef).
- **Subnet Mask (IPv4) or Prefix Length (IPv6):** Specify an appropriate subnet mask for IPv4 interface or prefix length for IPv6 interface. The prefix length ranges from 2 to 127.

Copyright ©2019, Infoblox, Inc. All right reserved.
**Gateway:** Type the IPv4 or IPv6 address of the default gateway depending on the type of interface. For IPv6 interface, you can also type Automatic to enable the appliance to acquire the IPv6 address of the default gateway and the link MTU from router advertisements.

**VLAN Tag:** For a VLAN, enter the VLAN tag or ID. You can enter a number from 1 to 4094. Ensure that you configure the corresponding switch accordingly.

**Port Settings:** From the drop-down list, choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose Full for concurrent bidirectional data transmission or Half for data transmission in one direction at a time. Select Automatic to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOS appliances.

**DSCP Value:** Displays the Grid DSCP value, if configured. To modify, click Override and enter the DSCP value. You can enter a value from 0 to 63. For information about DSCP, see Implementing Quality of Service Using DSCP.

---

**Note:** When the system operates in HA mode, should the IPv6–addressed VIP value be deleted, the IPv6 address of the HA port will also be deleted.

5. Optionally, define extensible attributes. For information, see Using Extensible Attributes.

6. Do one of the following:

- Click **Save & Edit** to add the HA member to the Grid and launch the editor. You can configure additional properties, such as the MTU size, or add the member to a NAT group.
- Click **Save & New** to add the HA member to the Grid and launch the wizard again to add another member.
- Click **Save & Close** to add the HA member to the Grid and close the wizard.

The communication protocol for all the services in a dual mode (IPv4 and IPv6) HA member is the same protocol as the one that is used for VRRP advertisements. For example, if you select IPv4 in the Send HA and Grid Communication over field in step 2 of the Add Grid Member wizard, then IPv4 is set as the communication protocol for all the services. However, you can override the communication protocol for all the services in a dual mode HA member. For information, see Changing the Communication Protocol for a Dual Mode Appliance.

### Changing the Member Type

When you change the Member Type from Infoblox to Virtual NIOS, Infoblox displays an error indicating that the network port of a vNIOS member must be set to Automatic. If you encounter this error, follow the steps mentioned below to change the Member Type to Virtual NIOS:

1. From the Grid tab, select the Grid Manager tab -> Members tab.
2. Expand the Toolbar and click Add -> Add Grid Member.
3. In the Add Grid Member wizard, leave the Member Type as Infoblox, fill other details and click Next.
4. In the Network tab select High Availability Pair.
5. Change the port settings to Automatic for Node1 HA.
6. Select Standalone Member.
7. Click Previous and change the Member Type to vNIOS.

### Changing the Communication Protocol for a Dual Mode Appliance

You can change the default communication protocol for a dual mode appliance. You can force the appliance to use a specific protocol to join the Grid Master and for the reporting services. But for services with two types of resolution (A and AAAA records), you can set the preferred communication protocol.

To change the communication protocol for a dual mode appliance:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> member check box -> Edit icon.
2. In the Grid Member Properties editor, select the Network tab -> Basic tab, and then complete the following:
   - **Communication Protocol Settings and Preferences:** This setting is not applicable for an HA pair. Select either IPv4 or IPv6 from the drop-down list. This setting will force the appliance to use the specified protocol for Grid and reporting services and this is the preferred protocol for services with two types of resolution (A and AAAA records).
   - **Customized Settings:** Select this and do the following:
     - **Always use this Communications Protocol for:** For a Grid Master, you can select either IPv4 or IPv6 from the Reporting drop-down list. This setting will force the Grid Master to use the specified communication protocol for reporting service. For a Grid member, you can select either IPv4 or IPv6 from the Grid and Reporting drop-down list. This setting will force the Grid member to use the specified communication protocol for Grid and reporting service.
     - **Always Prefer this Communications Protocol for:** This field lists the services which has two types of resolution (A and AAAA records). Select either IPv4 or IPv6 from the drop-down list for the service which you want the appliance to use this as the preferred communication protocol. The appliance uses the preferred protocol first for the service.

### Joining Appliances to the Grid

Grid members can join the Grid using IPv4 protocol in an IPv4-only Grid and using IPv6 protocol in an IPv6-only Grid. In a dual mode Grid, the Grid members may join the Grid using IPv4 or IPv6. Similarly, a Grid Master candidate can join the Grid using IPv4 in an IPv4-only Grid and using IPv6 in an IPv6-only Grid. But for a Grid Master candidate to join a dual mode Grid, it should be configured in dual mode. If you have configured the MGMT port for the Grid member, then the Grid member can join the Grid using the MGMT port. You can use the Grid Setup Wizard or access...
the Join Grid dialog box to join appliances to a Grid. The Grid Setup Wizard launches when you first log in to an appliance. You can also launch it from the Toolbar as described in Grid Setup Wizard.

To join a single appliance and HA pair to a Grid using the Grid Manager GUI:

1. Log in to the appliance or HA pair that you want to add to the Grid. The appliance or HA pair must be online and able to reach the Grid Master.
2. From the Grid tab, select the Grid Manager tab -> Members tab.
3. Expand the Toolbar and click Join Grid.
4. In the JoinGrid dialog box, enter the following:
   - **Virtual IP of Grid Master**: Type the VIP address of the HA Grid Master or the LAN1 address of the single Grid Master for the Grid to which you want to add the appliance. Entries may be an IPv4 or IPv6 address.
   - **Grid Name**: Type the name of the Grid.
   - **Grid Shared Secret**: Type the shared secret of the Grid.
   - **Use MGMT port to join Grid**: If you have already enabled the MGMT port (see Grid Communications), this option becomes available. Select it to connect to the Grid through the MGMT port.
5. Click OK to begin the join operation.

To confirm that the appliance has successfully joined the Grid, log in to the Grid Master and navigate to the Grid tab, select the Grid Manager -> Members tab. This panel lists the Grid members. Check the icon in the Status column of the newly added member. (green = the appliance has joined the Grid and is functioning properly; yellow = the appliance is in the process of joining the Grid; red = the appliance has not joined the Grid). You can also use the CLI command set network to join an appliance to a Grid.

To join a single appliance and HA pair to a Grid using the Grid Setup Wizard:

1. Log in to the appliance or HA pair that you want to add to the Grid. The appliance or HA pair must be online and able to reach the Grid Master.
2. From the Grid tab, select the Grid Manager tab -> Members tab.
3. Expand the Toolbar and click Grid Properties -> Setup (Grid Setup Wizard).
4. On the next screen, specify the Grid properties and click Next
   - **Grid Name**: Enter a text string that the two appliances use to authenticate each other when establishing a VPN tunnel between them. This must match the Grid name you entered for node 1.
   - **Grid Master’s IP Address**: Enter the same VIP you entered for node 1.
   - **Shared Secret**: Enter a text string that both appliances use as a shared secret to authenticate each other when establishing a VPN tunnel between them. This must match your entry in node 1.
5. On the next screen verify the IP address settings of the member and click Next.
6. The last screen displays the settings you specified in the previous panels of the wizard. Verify that the information is correct and click Finish.

To confirm that the appliance has successfully joined the Grid, log in to the Grid Master and navigate to the Grid tab, select the Grid Manager -> Members tab. This panel lists the Grid members. Check the icon in the Status column of the newly added member. (Green = The appliance has joined the Grid and is functioning properly; Yellow = The appliance is in the process of joining the Grid; Red = The appliance has not joined the Grid). You can also use the CLI command set network to join an appliance to a Grid.

**Grouping Members by Extensible Attributes**

When you have a few members in your Grid, you can organize and group them by extensible attributes that contain the same values. Using the Group Results function, you can organize your members in a meaningful way and quickly identify them based on common data. When you group members by multiple extensible attributes, the appliance groups the members hierarchically based on the order of the filters. For example, when you filter members first by extensible attribute “Site equals London” and then by extensible attribute “Organization equals Engineering,” the appliance groups corresponding members first by Site and then by Organization based on the values you enter. In the Grid tab -> Grid Manager tab -> Members tab, Grid Manager displays the grouped members in a hierarchical view that displays the member group name (London). You can click the London link and drill down to the next level of grouping. In this case, Grid Manager displays the organization group (Engineering) in the Members tab. When you click the Engineering link to drill down to the next level, all associated members that belong to this member group (London) -> Engineering) are displayed.

To go back to a previous hierarchical view, click the link of the corresponding level in the breadcrumb. To group members by extensible attributes:

1. From the Grid tab, select the Grid Manager tab -> Members tab.
   or From the Grid tab, select the Grid Manager tab -> Services tab.

   **Note**: You can use the “Group Results” function for the following services: DNS, DHCP, TFTP, FTP, HTTP, NTP, bloxTools, Captive Portal, and Reporting services.

   or From the Data Management tab, select the DHCP, File Distribution, or DNS tab -> Members/Servers tab.

2. Complete the following to group members with the same extensible attribute value:
   - **Group Results**: Select this check box to enable the appliance to group members by extensible attributes.
   - **Group By**: From the drop-down list, select the first extensible attribute that you want the appliance to use for filtering members.

Grid Manager displays data per group of members configured with the same extensible attribute value. To add additional Group By filter, click the + icon, and then select a value from the drop-down list. You can apply up to 10 Group By filters. You can also delete a filter by clicking the - icon.
When you enable reporting service on the Grid and configure multi-site cluster, you can group reporting members by reporting site extensible attributes. For information about reporting clusters, see Configuring Reporting Clusters.

Grid Manager displays the following information for the specified extensible attribute:

- `<Selected extensible attribute>`: Displays the extensible attribute value.
- `Status`: This is the overall status for all members in the group. Depending on the status of each member, the overall status can be one of the following: Working, Warning, Failed, Offline, Inactive, or Unknown. For information about the status, see Grid Status.

**Note:** In an HA pair, when one of the appliances is in the Working status and the other appliance has a status other than Working, Inactive, and Unknown, then the overall status of HA members is Warning. When you use filters and the group by extensible attribute feature, filters take precedence over the group by function.

When you drill-down to the member level, Grid Manager displays the members in the group.

**Configuring an IPv6-only Grid**

An IPv6-only Grid uses IPv6 as the communication protocol and it includes an IPv6 Grid Master and the Grid members, which can be either IPv6 or dual mode (IPv4 and IPv6). In order to configure an IPv6-only Grid, you have to first create an IPv6 Grid Master and then join the Grid members using their IPv6 addresses.

The process of configuring an IPv6-only Grid involves the following steps:

1. Make a console connection to the Grid Master and configure an IPv6 address for the Grid Master using the CLI command set network. For information, see Method 2 – Using the CLI.
2. Open a web browser and make an HTTPS connection to the IPv6 address of LAN1 port of the Grid Master.
3. Log in using the default user name and password `admin` and `infoblox`. For detailed information about logging in to the GUI, see Logging in to the GUI.
4. The Grid Setup Wizard appears when you first log in to the appliance. You can use it to create an IPv6 HA Master or IPv6 single Grid Master. For information about creating an HA Master, see Creating an HA Grid Master and for information about creating a single Grid Master, see Creating a Single Grid Master.

   The type of network connectivity for the Grid Master should be set to IPv6. To verify, navigate to the Grid tab -> Grid Manager tab -> Members tab -> member check box -> Edit icon. In the Grid Member Properties editor, select the Network tab -> Basic tab, check that the Type of Network Connectivity is set to IPv6. The Grid members can join the Grid Master using IPv6 only.

   **Note:** You can add additional IPv4 and IPv6 addresses for LAN2 and MGMT ports for the Grid services, in the Additional Ports and Addresses table. But for an IPv6-only Grid, you can configure IPv6 address for the VLAN port.

5. Add IPv6 single members and HA members to the Grid. For information, see Adding Grid Members.
6. You can use the Grid Setup Wizard or access the Join Grid dialog box to join appliances to a Grid. See Joining Appliances to the Grid.

You can also configure IPv6 address for the MGMT interface of the appliance and join the Grid through the MGMT interface.

**Transforming to an IPv6-only Grid**

After an upgrade from a previous NIOS release to NIOS 7.0 or later, each node in the Grid is set to either IPv4 or dual mode (IPv4 and IPv6). Transforming an IPv4-only Grid to an IPv6-only Grid may take a longer duration. Hence, before removing the IPv4 addresses from each Grid member, you have to configure additional IPv6 Grid communication protocol for each Grid member so that all the services function properly using IPv6.

Note the following before converting an IPv4-only or a dual mode Grid to an IPv6-only Grid:

- If a Grid member is designated as a Master Candidate, the Grid manager does not allow you to change the type of network connectivity of the Grid Master or the Grid Master Candidate. Therefore, you must disable the Grid member from being a Grid Master Candidate before changing the type of network connectivity of the Grid Master or the Grid Master Candidate. You can deselect the Master Candidate option in the General tab of the Grid Member Properties editor to disable a member from being a Master Candidate. Note that at this point, the Grid will not have a Grid Master Candidate and this may result in an unrecoverable condition, if the Grid Master goes down.
- You must stop all services on the Grid Master and Grid members that uses IPv4.
- If external servers like authentication servers, forwarders, root name servers, backup servers, etc. is configured with IPv4 addresses, then it will not work after converting the Grid to an IPv6-only Grid. Hence, make sure that you change the IPv4 address of the external server to IPv6 address before converting the Grid to an IPv6-only Grid.

**Note:** Infoblox recommends that you backup the configuration after you convert a Grid to IPv6-only mode. Restoring the old backup by performing a forced restore, may prevent the Grid members from rejoining the Grid Master after the restore.

The process of transforming an IPv4-only or dual mode Grid to an IPv6-only Grid involves the following steps:

1. **Convert the Grid Master into dual mode (IPv4 and IPv6):**
   - Login to the Grid Master, from the Grid tab -> Grid Manager tab -> Members tab -> select the Grid Master and click the Edit icon.
   - In the Grid Member Properties editor, select the Network tab -> Basic tab.
   - In the Type of Network Connectivity field, select IPv4 and IPv6 from the drop-down list and enter the network information for LAN1 (IPv6) address in the Ports and Addresses table.

Copyright ©2019, Infoblox, Inc. All right reserved.
For HA Master, select IPv4 in the Send HA and Grid Communication Over field, and enter the network information for VIP (IPv6), Node1 LAN1 (IPv6), Node2 LAN1 (IPv6) in the Ports and Addresses table.

- Save the configuration and click Restart if it appears at the top of the screen.

2. Similarly, convert all the Grid members into dual mode (IPv4 and IPv6) if it is in IPv4 mode. All the members will rejoin the Grid using IPv4.

3. Force each Grid member to rejoin the Grid using IPv6, as follows:
   - From the Grid tab, select the Grid Manager tab -> Members tab -> member check box -> Edit icon.
   - In the Grid Member Properties editor, select the Network tab -> Basic tab.
   - In the Always Force or Prefer this Communications Protocol field, select IPv6 from the drop-down list and also select IPv6 in the Send HA and Grid Communication over field if the member is an HA pair.

   This setting will force the Grid member to rejoin the Grid using IPv6 and it uses IPv6 for all the services.

   - Save the configuration and click Restart if it appears at the top of the screen.

4. Configure each Grid member to provide DNS service using IPv6, as follows:
   - From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon.
   - In the Member DNS Properties editor, select the General tab -> Basic tab.
   - Enable the IPv6 check box for the desired interface (LAN1, LAN2, or MGMT) under DNS Interfaces.

   Ensure that the primary and secondary servers are configured with an IPv6 address for each zone, before disabling the IPv4 check box for LAN1, LAN2, or MGMT interface.

   - Save the configuration and click Restart if it appears at the top of the screen.

Note: When you transform an IPv4-only or dual mode Grid to an IPv6-only Grid, the LAN1 port for IPv4 is always enabled. The LAN1 port is disabled only when the Grid is configured using IPv6 from the beginning.

5. Configure each Grid member to provide DHCP service using IPv6, as follows:
   - From the Data Management tab, select the DHCP tab -> Members tab -> member check box -> Edit icon.
   - In the Member DHCP Properties editor, select the General tab -> Basic tab.
   - Disable the IPv4 check box for LAN1 and LAN2 interface under DHCP Interfaces.

   If IPv6 network is not configured, you can create an IPv6 network. For information, see Managing IPv6 Networks.

   - Enable the IPv6 check box for the desired interface (LAN1 or LAN2) under DHCP Interfaces.

   - Save the configuration and click Restart if it appears at the top of the screen.

6. Enable each Grid member and the Grid Master to use IPv6 for all the services, as follows:
   - From the Grid tab, select the Grid Manager tab -> Members tab -> member check box -> Edit icon.
   - In the Grid Member Properties editor, select the Network tab -> Basic tab, and select Customized Settings and specify the following:
     - Always Force this Communication Protocol for: Select IPv6 from the drop-down list for the Grid and reporting service.
     - Always Prefer this Communication Protocol for: Select IPv6 from the drop-down list as the preferred communication protocol for the listed services which has two types of resolution (A and AAAA records). The appliance uses the preferred protocol first for the service.

   - Save the configuration and click Restart if it appears at the top of the screen.

7. When all the services are functioning using IPv6, you can remove the IPv4 addresses from all the Grid members by converting the Grid member from dual mode (IPv4 and IPv6) to IPv6 mode, as follows.

   - From the Grid tab, select the Grid Manager tab -> Members tab -> member check box -> Edit icon.
   - In the Grid Member Properties editor, select the Network tab -> Basic tab.

   - In the Type of Network Connectivity field, select IPv6 from the drop-down list.

   - Save the configuration and click Restart if it appears at the top of the screen.

8. Similarly, you can convert the Grid Master from dual mode (IPv4 and IPv6) to IPv6 mode after converting all the Grid members to IPv6.

   - From the Grid tab, select the Grid Manager tab -> Members tab -> member check box -> Edit icon.
   - In the Grid Member Properties editor, select the Network tab -> Basic tab.

   - In the Type of Network Connectivity field, select IPv6 from the drop-down list.

   - Save the configuration and click Restart if it appears at the top of the screen.

   - In the Type of Network Connectivity field, select IPv6 from the drop-down list.

   - Save the configuration and click Restart if it appears at the top of the screen.

Note: Remove the IPv4 addresses from the Grid Master only after you remove the IPv4 addresses from all the Grid members.

Auto-Provisioning NIOS Appliances

In addition to using the Grid Setup Wizard or access the Join Grid dialog box to join appliances to a Grid, you can set up an appliance using the auto-provisioning feature, which allows a DHCP server to automatically assign an IP address to the appliance. You can then join the auto-provisioned appliance to the Grid.

Auto-provisioning is enabled by default for new installations of physical appliances, but it is not supported for vNIOS appliances. When you connect the appliance to the network, a lease request is automatically sent to the DHCP server. The DHCP server fingerprints the client as "Infoblox Appliance," as the DHCP client provides the unique option sequence (1,28,2,2,3,3,15,6,12) and vendor ID (INFOBLOX). The DHCP server assigns a DHCP lease and a dynamic IP address to the appliance. If the DHCP lease request fails, the default IP address (192.168.1.2) is assigned to the appliance. The DHCP client tries to send the lease request for a duration of one minute when the appliance is either in the factory default state or in the auto-configured default IP address state after a reboot. If you do not use auto-provisioning to set up the appliance, then you can wait one minute before connecting the appliance to the network. Otherwise, the DHCP server will assign a dynamic IP address to the appliance. Note that if you have already set the IP address for the appliance through the Infoblox CLI, GUI, or API, then auto-provisioning is disabled for the appliance and the lease address is not requested. When auto-provisioning is enabled for an appliance, the DNS, DHCP, FTP, TFTP, HTTP, NTP, bloxTools, Captive Portal, Reporting services, as well as backup and restore are disabled for the member until a static IP address is set for the appliance. You can join a single appliance or HA pair to the Grid. After the appliance joins the Grid, the static IP address is set for the appliance.

Note: Auto-provisioning supports only IPv4 addressing and not IPv6 addressing.
Setting Up Physical Appliances Using Auto-Provisioning

Complete the following to set up an appliance using auto-provisioning and to join the auto-provisioned appliance to the Grid Master:

1. Connect the appliance to a network using an Ethernet cable, connect it to a power source, and then turn on the power. For information about cabling the appliance to a network and powering the appliance, refer to the user guide or installation guide that ships with the product.
   A lease request is automatically sent to the DHCP server that assigns a DHCP lease and a dynamic IP address to the appliance. The DHCP client tries to send the lease request for a duration of one minute and if the request fails, the default IP address (192.168.1.2) is assigned to the appliance.
2. Join the appliance to the Grid Master. You can join the auto-provisioned appliance to the Grid Master using the Connect dialog box. For more information, see Joining Appliances to the Grid. A static IP address is set and auto-provisioning is automatically disabled for the appliance after it joins the Grid.

Note: When auto-provisioning is disabled for an appliance and the network address is not preserved, auto-provisioning will be re-enabled and a DHCP lease request sent to the DHCP server if you reset the appliance using the CLI command reset all auto_provision or reset the database using the CLI command reset database auto_provision. However, if the static IP address for an appliance is set and network settings are preserved, auto-provisioning will be re-enabled for the appliance but the lease address will not be requested if you reset the database using the CLI command reset database auto_provision.

Joining Auto-Provisioned Appliances to the Grid

You can join a predefined appliance with a DHCP lease to the Grid Master using the Connect dialog box. You can join a single appliance or an HA pair to the Grid Master. For an HA pair, the member which is offline will join the Grid Master and it will become the active node. When both the members of an HA pair are offline, Node 1 of an HA pair is joined to the Grid Master.
Only superusers can join a Grid member to the Grid Master. If the Grid member fails to join the Grid, then the remote console is enabled for the appliance and you can join the appliance to a Grid through the remote console. You can log in to the remote console using the user name, admin and the Grid shared secret as the password.
To join a single appliance or an HA pair to a Grid Master, complete the following:

1. Log in to the Grid Master. Note that the single appliance or the HA pair must be online and the Grid Master must be able to reach the appliance.
2. From the Grid tab, select the Grid Manager tab -> Members tab.
3. Add the appliance as a Grid member. For information about adding Grid members to the Grid, see Adding Grid Members.
4. Select the Grid member that you want to join to the Grid Master, expand the Toolbar and click Connect.
5. The following fields are displayed in the Connect dialog box:
   - **Host Name**: The name of the member.
   - **Configured IPv4 Address**: The IPv4 address of the member.
   - **Site**: The site to which the IP address belongs. This is one of the predefined extensible attributes.
   - **Temporary IPv4 Address**: Enter the IPv4 address of the DHCP lease or click Select to select the DHCP lease.
     Grid Manager displays the Lease Selector dialog box from which you can select the DHCP lease. Note that the Lease Selector displays the active DHCP leases which are fingerprinted as “Infoblox Appliance”.
6. Click Next to retrieve the appliance information.
   The Grid Master uses SSL to connect to the appliance and it gets the appliance information. Grid Manager displays the following information for the appliance:
   - **Remote Appliance Type**: The appliance type.
   - **Remote Appliance Serial Number**: The serial number of the appliance.
   - **Licenses**: Grid Manager displays the Grid license and the licenses that are pre-provisioned on the member. It displays the following information:
     - **Type**: The license type.
     - **String**: The license string. If the license string is not displayed, you can enter or paste it here.
7. Click Connect to join the appliance to the Grid Master.
   To confirm that the appliance has successfully joined the Grid, check the status in the Status column of the newly added member. (Green = The appliance has joined the Grid Master and is functioning properly; Yellow = The appliance is in the process of joining the Grid Master; Red = The appliance has not joined the Grid Master).

Pre-Provisioning NIOS and vNIOS Appliances

Before joining a member to the Grid, you can first enable provisional licenses and make necessary configurations on the offline member, which allows DNS and DHCP data to be associated with the member prior to its deployment. Note that pre-provisioned members are treated as offline members. There are a few guidelines to consider before you pre-provision a member. For more information about the guidelines, see 4823797 48 23797.
When you add a new member to the Grid, the Pre-Provisioning tab is displayed in the Grid Member Properties editor. You can pre-provision the member by defining its hardware model and enable certain provisional licenses through the Pre-Provisioning tab. This tab is not displayed after the member successfully joins the Grid. NIOS supports the following provisional licenses: Cloud Platform, DHCP, DNS, DNS Traffic Control,
Enterprise (formerly Grid), FireEye, Microsoft Management, RPZ (Response Policy Zone), and vNIOS. You must enable provisional licenses before you can make supported configurations on the pre-provisioned member. For more information about these licenses, see 4823797.

**Note:** You must have the Enterprise and vNIOS licenses pre-provisioned in order for a vNIOS appliance to join the Grid. For a cloud virtual appliance, include the Cloud Platform license.

To pre-provision an offline Grid member and join it to the Grid at a later time, complete the following:

1. Add a new single member or HA member to the Grid, as described in Adding a Single Member or Adding an HA Member.
2. Pre-provision the offline member, as described in 4823797.
3. Configure services to use the pre-provisioned member.
4. Obtain permanent licenses you have specified for pre-provisioning and use the `set license` CLI command to install the licenses on the member. For more information about CLI commands, refer to the Infoblox CLI Guide.
5. Join the pre-provisioned member to the Grid, as described in Joining Appliances to the Grid. For guidelines about joining pre-provisioned members, see 4823797 4823797.

### Guidelines for Pre-provisioning Offline Grid Members

Before you pre-provision a Grid member, consider the following:

- A pre-provisioned Grid member is an offline member. When you upgrade a Grid that has a pre-provisioned member, the upgrade behaves the same way as it does when you upgrade the Grid that has an offline member. Note that you cannot pre-provision a member or update its settings during a scheduled upgrade. For more information about upgrades, see About Upgrades.
- You cannot change the pre-provisioned member configuration after you save it. To change the configuration, you first must delete the member and pre-provision it again. If you want to delete certain provisional licenses or change the hardware model for the pre-provisioned member, you must also first delete the existing member and define a new one. For information about deleting a member, see Removing a Grid Member.
- When you assign a network, zone, or IPv4 DHCP failover association to a pre-provisioned member, the Restart Service button is not displayed. If you restart any service on a pre-provisioned member, no action is actually taken even though you may receive a message indicating that the operation may take a few minutes. When you join the member to the Grid, NIOS will run respective member services on the joined member. For more information about service restarts, see Restarting Services.
- NIOS allows you to backup information about the pre-provisioned member. When you perform a forced restore however, NIOS does not restore the pre-provisioned licenses if you have already installed permanent NIOS licenses on the corresponding member. For more information about backup and restore, see Backing Up and Restoring Configuration Files.
- You can use Manage Member Services to manage the pre-provisioned member services. For more information, see Monitoring Member Services.

### Configuring Pre-Provisioned Members

The pre-provisioning feature is disabled by default. You must select a supported hardware model for the member to enable this feature.

To pre-provision an offline member, login to the Grid Master and complete the following:

1. From the Grid tab, select the Grid Manager tab -> Members tab, and then click the Add icon.
2. In the Add Grid Member wizard, add a new member as described in Adding a Single Member.
3. After you add the member to the Grid, select the member in the Members tab and click the Edit icon.
4. In the Grid Member Properties editor, select the Pre-Provisioning tab, and complete the following:
   - **Member Type:** Displays the member type that you have selected in the General tab. The pre-provisioning feature is supported only for Infoblox and Virtual NIOS member types. Note that you must select a hardware model for the member in order to enable the pre-provisioning feature.
   - **Hardware Model:** Select the hardware model from the drop-down list. Grid Manager displays only the supported hardware models for the specified member type. Once you select the hardware model, the pre-provisioning feature is enabled for the member. NIOS allows you to pre-provision HA members that have the same or different hardware models for Node 1 and Node 2. A few hardware specific features, such as DSCP, VLAN, LAN2, and LOM (Light Out Management), are enabled based on the pre-provisioned hardware model you specify here.
   - **Provisional Licenses:** Select the licenses that you want to enable for the pre-provisioned member. You can select the licenses only after you have specified the hardware model for the member. Once you select and enable a license, you can no longer modify the hardware model for the member. Note that the permanent licenses that you later add to the member must include the ones that are specified for pre-provisioning.
5. Save the configuration.

**Note:** After you save the configuration, you can no longer modify the hardware model for the member. You also cannot disable any provisional licenses, though you can add new ones. To disable provisional licenses, you must first remove the pre-provisioned member and then configure a new one.

### About Provisional Licenses

Copyright ©2019, Infoblox, Inc. All right reserved.
If a member has never joined a Grid, you can pre-provision this member provided that you define the hardware model for the member and assign provisional licenses to it. Provisional licenses are not permanent NIOS licenses. Though they do not have expiration dates or validity periods, you must replace these licenses with corresponding permanent licenses before you join the member to the Grid.

Note: Before you join the member to the Grid, use the CLI command `set license` to add corresponding permanent licenses that you have specified for pre-provisioning. For information about CLI commands, refer to the Infoblox CLI Guide. You can also allocate pre-purchased licenses from the pool. For information, see You can use the following OpenStack cloud-init template to configure an IB-V815 as a Grid Master.

NIOS supports the following provisional licenses: Cloud Platform, DHCP, DNS, DNS Traffic Control, Enterprise (formerly Grid), FireEye, Microsoft Management, RPZ (Response Policy Zone), and vNIOS.

After you configure the offline member, you can select the pre-provisioned member from the corresponding wizards and editors based on the required license(s). The following table lists the wizards and editors from which you can select a pre-provisioned member when required pre-provisioned licenses are enabled:

<table>
<thead>
<tr>
<th>Wizards and editors from which you can select a pre-provisioned member</th>
<th>Required license(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Zones and Name Server Groups</td>
<td>dns</td>
</tr>
<tr>
<td>DHCP IPv4 and IPv6 networks</td>
<td>dhcp</td>
</tr>
<tr>
<td>IPv4 DHCP Failover Association</td>
<td>dhcp</td>
</tr>
<tr>
<td>Microsoft servers</td>
<td>ms_management</td>
</tr>
<tr>
<td>Note that the initial synchronization with Microsoft servers is read-only. When you join the appliance to the Grid, the appliance removes all Microsoft management objects that you have configured on the Microsoft servers after the synchronization. The configuration on the Microsoft servers will replace the configuration on the NIOS appliance.</td>
<td></td>
</tr>
<tr>
<td>Grid Members</td>
<td>vnios</td>
</tr>
<tr>
<td>Grid license</td>
<td>enterprise</td>
</tr>
<tr>
<td>Response Policy Zones</td>
<td>RPZ</td>
</tr>
<tr>
<td>Response Policy Zones</td>
<td>FireEye</td>
</tr>
<tr>
<td>DNS Traffic Control</td>
<td>DTC</td>
</tr>
<tr>
<td>Cloud tabs and related wizards and editors</td>
<td>cloud_api</td>
</tr>
</tbody>
</table>

Note: If you configure a DHCP Failover using an online member and a pre-provisioned member, assign it to a range, and start DHCP service, no addresses will be served because the initial synchronization does not happen due to the pre-provisioned offline member. NIOS logs the following message in the syslog:

```
2013-12-24T08:37:23+00:00 daemon (none) dhcpd[8790]: info DHCPDISCOVER from cb:86:a8:45:6c:5c via 10.120.21.236: not responding (recovering)
```

Guidelines for Joining Pre-Provisioned Members to the Grid

Before you join a pre-provisioned member to the Grid, ensure that you verify the appliance model and provisional licenses for the member. For information about how to join a member to the Grid, see Joining Appliances to the Grid.

Note the following about joining a pre-provisioned member to the Grid:

- If you install fewer permanent licenses than the specified provisional licenses, you cannot join the member to the Grid.
- If the pre-provisioned member does not have any provisional licenses enabled, you can join the member to the Grid provided that you install a permanent Grid license on the member.
- You must install at least the set of permanent licenses that were specified for pre-provisioning along with any other needed licenses, except for the following:
  - You can join the member to the Grid if the pre-provisioned member is a vNIOS virtual appliance and has only the DNS license enabled, and you install both the vNIOS and DNS licenses on the member.
  - Similarly, you can join the member to the Grid if the pre-provisioned member is a vNIOS virtual appliance and has both DNS and DHCP licenses enabled, and you install the vNIOS, DNS, and DHCP licenses on the member.
- After you successfully join the pre-provisioned member to the Grid, provisional licenses are removed and permanent licenses take effect.
- After the member joins the Grid successfully, the Pre-Provisioning tab is not displayed in the Grid Member Properties editor.

Configuration Example: Configuring a Grid
You can configure an IPv4-only, IPv6-only, or a dual mode (IPv4 and IPv6) Grid, but the configuration example uses IPv4 addresses. In this example, you configure seven NIOS appliances in a Grid serving internal DHCP and DNS for an enterprise with the domain name corpxyz.com. There are four sites: HQ and three branch offices. A hub-and-spoke VPN tunnel system connects the sites, with HQ at the hub. The distribution and roles of the NIOS appliances at the four sites are as follows:

- HQ site (four appliances in two HA pairs):
  - HA Grid Master – hidden primary DNS server
  - HA member – secondary DNS server and DHCP server for HQ
- Site 1 (two appliances in an HA pair): HA member – secondary DNS server and DHCP server for Site 1
- Site 2 (one appliance): single member – secondary DNS server and DHCP server for Site 2

**Note:** When adding an Infoblox appliance to an existing Grid, you must first check whether the Grid is running the minimum required software release of the appliance. For information, refer to the document, *Minimum Required Release Software for Hardware Platforms*, that was shipped with your product.

To create a Grid, you first create a Grid Master and then add members. The process involves these three steps:

1. Configuring two appliances at HQ as the Grid Master. See [Create the Grid Master](#).
2. Logging in to the Grid Master and defining the members that you want to add to the Grid; that is, you configure Grid member settings on the Grid Master in anticipation of later joining those appliances to the Grid. See [Define Members on the Grid Master](#).
3. Logging in to the individual appliances and configuring them so that they can reach the Grid Master over the network and join the Grid. See [Join Appliances to the Grid](#).

After creating the Grid and adding members, you use the Data Import Wizard to import DHCP and DNS data from legacy servers. See [Import DHCP Data](#) and [Import DNS Data](#).

Finally, you transition DHCP and DNS service from the legacy servers to the Infoblox Grid members. See [Enable DHCP and Switch Service to the Grid](#).

*Figure 5.16 Network Diagram*
Cable All Appliances to the Network and Turn On Power

Cable the NIOS appliances to network switches. After cabling each appliance to a switch and connecting it to a power source, turn on the power. For information about installing and cabling the appliance, refer to the user guide or installation guide that ships with the product.

1. At HQ and Site 1, connect Ethernet cables from the LAN1 and HA ports on the appliances in each HA pair to a switch, connect the appliances to power sources, and turn on the power for each appliance.

   **Note:** When connecting the nodes of an HA pair to a power source, connect each node to a different power source if possible. If one power source fails, the other might still be operative.

2. At Site 2, connect an Ethernet cable from the LAN1 port on the single appliance to a switch, connect the appliance to a power source, and turn on the power for that appliance.

Create the Grid Master

**Note:** IPv6 addressing is fully supported on Infoblox Grid Masters, HA pairs and standalone HA pairs and appliances. Examples in the sections of this chapter use IPv4.

Configure two appliances at HQ to be the two nodes that make up the HA pair forming the Grid Master.

**Grid Master – Node 1**

1. By using the LCD or by making a console connection to the appliance that you want to make Node 1 of the HA pair for the Grid Master, change the default network settings of its LAN1 port to the following:
   - IP Address: 10.0.1.6
   - Netmask: 255.255.255.0
   - Gateway: 10.0.1.1

2. Connect your management system to the HQ network, open a browser window, and connect to [https://10.0.1.6](https://10.0.1.6).

3. Log in using the default user name and password admin and infoblox.


5. On the first screen, select *Configure a Grid Master* and click *Next*.

6. Specify the Grid properties:
   - **Grid Name:** Enter corpxyz.
   - **Shared Secret:** Enter Mg1kW17d.
   - **Confirm Shared Secret:** Enter Mg1kW17d.
   - **Hostname:** Enter ns1.corpxyz.com.
   - **Type of Network Connectivity:** Select *IPv4* from the drop-down list.
   - **Is the Grid Master an HA pair?** Select *Yes*.

7. Specify the network properties and click *Next*:
   - **Virtual Router ID:** Enter 143.
   - **Required Ports and Addresses:** Enter the following to set up the HA pair:

     | Interface  | Address     | Subnet Mask (IPv4) or Prefix Length (IPv6) | Gateway | Port Settings |
     |------------|-------------|---------------------------------------------|---------|---------------|
     | VIP (IPv4) | 10.0.1.10   | 255.255.255.0                               | 10.0.1.1| Automatic     |
     | Node1 HA (IPv4) | 10.0.1.7   | 255.255.255.0                               | 10.0.1.1| Automatic     |
     | Node2 HA (IPv4) | 10.0.1.9   | 255.255.255.0                               | 10.0.1.1| Automatic     |
     | Node1 LAN1 (IPv4) | 10.0.1.6   | 255.255.255.0                               | 10.0.1.1| Automatic     |
     | Node2 LAN1 (IPv4) | 10.0.1.8   | 255.255.255.0                               | 10.0.1.1| Automatic     |

8. Enter a new password: 1n85w2IF. Retype it and click *Next*.

9. Complete the following:
   - **Time zone:** Select (UTC – 8:00 Pacific Time (US and Canada), Tijuana
   - **Enable NTP:** click the Add icon and enter the IP address of the NTP server: 10.120.3.10

10. Click *Finish*.

   When you click Finish, the Infoblox GUI application restarts.

**Grid Master – Node 2**

1. By using the LCD or by making a console connection to the appliance that you want to make Node 2 of the HA pair for the Grid Master, change the default network settings of its LAN1 port to the following:
IP Address: 10.0.1.8  
Netmask: 255.255.255.0  
Gateway: 10.0.1.1  

1. In the login window, type 10.0.1.8 in the Hostname field.  
2. Log in using the default user name and password admin and infoblox.  
3. From the Grid tab, select the Grid Manager tab -> Members tab -> member check box.  
4. Expand the Toolbar and click Join Grid and specify the following:  
   • Virtual IP of Grid Master: 10.0.1.10.  
   • Grid Name: Enter corpxyz.  
   • Grid Shared Secret: Enter Mg1kW17d.  
5. Confirm the configuration, and then on the last screen of the wizard, click Finish. The HTTPS session terminates, but the login window remains open.  
6. In the login window, type 10.0.1.10 (the VIP address for the Grid Master) in the Hostname field.  
7. Log in using the default user name admin and the password 1n85w2IF.  
8. To check the status of the two nodes of the HA Grid Master, navigate to the Grid tab, select the Grid Manager -> Members tab. This panel lists the Grid members. Check the icon in the Status column of the Grid Master. (green = the appliance has joined the Grid and is functioning properly; yellow = the appliance is in the process of joining the Grid; red = the appliance has not joined the Grid). You can also use the CLI command set network to join an appliance to a Grid. Check that the status indicators are all green in the Detailed Status panel.  

During the joining process, an appliance passes through the following four phases:  
1. Offline – the state when a Grid member—in this case, the second node of the HA pair composing the Grid Master—is not in contact with the active node of the master  
2. Connecting – the state when an appliance matching a member configuration contacts the master to join the Grid and negotiates secure communications and Grid membership  
3. Synchronizing – the master transmits its entire database to the member  
4. Running — the state when a member is in contact with the master and is functioning properly  

Note: Depending on the network connection speed and the amount of data that the master needs to synchronize with the member, the process can take from several seconds to several minutes to complete.  

Define Members on the Grid Master  

Before logging in to and configuring the individual appliances that you want to add to the Grid, define them first on the Grid Master. You can configure a Grid member in IPv4, IPv6, or a dual mode (IPv4 and IPv6), but the configuration example uses IPv4 addresses.  

HQ Site – HA Member  

1. From the Grid tab, select the Grid Manager -> Members tab.  
2. Expand the Toolbar and click Add -> Add Grid Member.  
3. In the Add Grid Member wizard, complete the following and click Next:  
   • Member Type: Select Infoblox.  
   • Host Name: Enter ns2.corpxyz.com.  
   • Comment: Enter HQ Site - ns2.corpxyz.com.  
4. Enter the following information about the member that you are adding to the Grid and click Save & Close:  
   • Type of Network Connectivity: Select IPv4 from the drop-down list.  
   • High Availability Pair: Select this option.  
   • Virtual Router ID: 210  
   • Required Ports and Addresses:  

<table>
<thead>
<tr>
<th>Interface</th>
<th>Address</th>
<th>Subnet Mask (IPv4) or Prefix Length (IPv6)</th>
<th>Gateway</th>
<th>Port Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP (IPv4)</td>
<td>10.0.2.10</td>
<td>255.255.255.0</td>
<td>10.0.2.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node1 HA (IPv4)</td>
<td>10.0.2.7</td>
<td>255.255.255.0</td>
<td>10.0.2.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node2 HA (IPv4)</td>
<td>10.0.2.9</td>
<td>255.255.255.0</td>
<td>10.0.2.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node1 LAN1 (IPv4)</td>
<td>10.0.2.6</td>
<td>255.255.255.0</td>
<td>10.0.2.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node2 LAN1 (IPv4)</td>
<td>10.0.2.8</td>
<td>255.255.255.0</td>
<td>10.0.2.1</td>
<td>Automatic</td>
</tr>
</tbody>
</table>

Site 1 – HA Member  

1. From the Grid tab, select the Grid Manager tab -> Members tab.  
2. Expand the Toolbar and click Add -> Add Grid Member.  
3. In the Add Grid Member wizard, enter the following and click Next:  
   • Member Type: Select Infoblox.
3. Specify the following information about the member that you are adding to the Grid and click Save & Close:
   - **Type of Network Connectivity**: Select IPv4 from the drop-down list.
   - **High Availability Pair**: Select this option.
   - **Virtual Router ID**: Enter 111.
   - **Required Ports and Addresses**:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Address</th>
<th>Subnet Mask (IPv4) or Prefix Length (IPv6)</th>
<th>Gateway</th>
<th>Port Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP (IPv4)</td>
<td>10.1.1.10</td>
<td>255.255.255.0</td>
<td>10.1.1.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node1 HA (IPv4)</td>
<td>10.1.1.7</td>
<td>255.255.255.0</td>
<td>10.1.1.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node2 HA (IPv4)</td>
<td>10.1.1.9</td>
<td>255.255.255.0</td>
<td>10.1.1.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node1 LAN1 (IPv4)</td>
<td>10.1.1.6</td>
<td>255.255.255.0</td>
<td>10.1.1.1</td>
<td>Automatic</td>
</tr>
<tr>
<td>Node2 LAN1 (IPv4)</td>
<td>10.1.1.8</td>
<td>255.255.255.0</td>
<td>10.1.1.1</td>
<td>Automatic</td>
</tr>
</tbody>
</table>

Site 2 – Single Member

1. From the **Grid** tab, select the **Grid Manager -> Members** tab.
2. Expand the Toolbar and click **Add -> Add Grid Member**.
3. In the **Add Grid Member** wizard, enter the following and click **Next**:
   - **Member Type**: Select Infoblox.
   - **Host Name**: ns4.site2.corpxyz.com
   - **Comment**: Site 2- ns4.site2.corpxyz.com
4. Specify the following information about the member that you are adding to the Grid and click **Next**:
   - **Type of Network Connectivity**: Select IPv4 from the drop-down list.
   - **Standalone Member**: Select this option.
   - **Required Ports and Addresses**: Click the empty fields and enter the following information:
     - **Address**: Enter 10.2.1.10.
     - **Subnet Mask (IPv4) or Prefix Length (IPv6)**: Enter 255.255.255.0.
     - **Gateway**: Enter 10.2.1.1.
     - **Port Settings**: Select AUTOMATIC.
5. Save the configuration and click **Restart** if it appears at the top of the screen.
6. Log out from the Grid Master.

Join Appliances to the Grid

To complete the process of adding appliances to the Grid, log in to and configure each individual appliance so that it can contact the Grid Master.

**HQ Site – HA Grid Member (Node 1)**

Make a console connection to the appliance that you want to make Node 1 in the HA pair, and enter the following:

```
Infoblox > set network
```

**NOTICE**: All HA configuration is performed from the GUI. This interface is used only to configure a standalone node or to join a Grid.

Enter IP address: 10.0.2.6
Enter netmask : 255.255.255.0
Enter gateway address : 10.0.2.1
Configure IPv6 network settings? (y or n):n Become Grid member? (y or n): y
Enter Grid Master VIP: 10.0.1.10
Enter Grid Name: corpxyz
Enter Grid Shared Secret: Mg1kW17d
New Network Settings: IP address: 10.0.2.6
Netmask: 255.255.255.0
Gateway address: 10.0.2.1
Join Grid as member with attributes: Grid Master VIP: 10.0.1.10
Grid Name: corpxyz
Grid Shared Secret: Mg1kW17d
WARNING: Joining a Grid will replace all the data on this node!
Is this correct? (y or n): y
Are you sure? (y or n): y
The Infoblox application restarts. After restarting, the appliance contacts the Grid Master and joins the Grid as Node 1.
HQ Site – HA Member (Node 2)

Make a console connection to the appliance that you want to make Node 2 in the HA pair, and enter exactly the same data you entered for Node 1 except that the IP address is 10.0.2.8.

After the application restarts, the appliance contacts the Grid Master and joins the Grid as Node 2, completing the HA member configuration for the HQ site.

Site 1 – HA Grid Member (Node 1)

Make a console connection to the appliance that you want to make Node 1 in the HA pair at Site 1, and use the set network command to configure its basic network and Grid settings. Use the following data:

- IP Address: 10.1.1.6
- Netmask: 255.255.255.0
- Gateway: 10.1.1.1
- Grid Master VIP: 10.0.1.10
- Grid Name: corpxyz
- Grid shared secret: Mg1kW17d

The Infoblox application restarts. After restarting, the appliance contacts the Grid Master and joins the Grid as Node 1.

Site 1 – HA Grid Member (Node 2)

Make a console connection to the appliance that you want to make Node 2 in the HA pair at Site 1, and enter exactly the same data you entered for Node 1 except that the IP address is 10.1.1.8.

After the application restarts, the appliance contacts the Grid Master and joins the Grid as Node 2, completing the HA member configuration for Site 1.

Site 2 – Single Grid Member

Make a console connection to the appliance that you want to make Node 1 in the HA pair at Site 1, and use the set network command to configure its basic network and Grid settings. Use the following data:

- IP Address: 10.2.1.10
- Netmask: 255.255.255.0
- Gateway: 10.2.1.1
- Grid Master VIP: 10.0.1.10
- Grid name: corpxyz
- Grid shared secret: Mg1kW17d

The Infoblox application restarts. After restarting, the appliance contacts the Grid Master and joins the Grid.

To check the status of all the Grid members, log in to the Grid Master at 10.0.1.10, and from the Grid tab, select the Grid Manager tab -> Members tab, select 10.0.1.10 and click the Detailed Status icon. Check that the status indicators are all green in the Detailed Status panel. As an appliance joins a Grid, it passes through the following phases: Offline, Connecting, (Downloading Release from Master), Synchronizing, and Running.)

**Note:** Depending on the network connection speed and the amount of data that the master needs to synchronize with the member, the process of joining a Grid can take from several seconds to several minutes to complete.

The Grid setup is complete.

Import DHCP Data

The Data Import Wizard is a software tool that you can download from the Infoblox Support site to your management system. With it, you can import data from legacy DHCP and DNS servers to NIOS appliances. In this example, you use it to import both DHCP and DNS data to the Grid Master at 10.0.1.10, which then uses the database replication mechanism to send the imported data to other Grid members. In the wizard, you also specify which Grid members serve the imported data. The wizard supports various types of DHCP formats, such as the following:

- ISC DHCP
- Lucent VitalQIP
- Microsoft
- Nortel NetID
- CSV (comma-separated values); you can also import IPAM data in CSV format In this example, all the DHCP data is in standard ISC DHCP format.
Importing DHCP Data for HQ and Site 2

1. Save the DHCP configuration file from your legacy DHCP server at 10.0.2.20 to a local directory.
2. Visit https://support.infoblox.com, log in with your support account, and download the Data Import Wizard. The Data Import Wizard application downloads to a container within a Java sandbox on your management system and immediately launches, displaying the Welcome page.
3. After reading the information in the left panel, click Next.
4. Select Import to Infoblox Appliance, enter the following, and then click Next:
   - Hostname or IP address: 10.0.1.10
   - Username: admin
   - Password: 1n85w2IF
5. Select the following, and then click Next:
   - Which kind of data would you like to import? DHCP/IPAM
   - Which legacy system are you importing from? ISC DHCP
   - Which appliance will be serving this data? 10.0.2.10
6. Type the path and file name of the DHCP configuration file saved from the legacy server, and then click Next.
   - or
   - Click Browse, navigate to the file, select it, click Open, and then click Next.
7. In the Global DHCP Configuration table, double-click the Value cell for the domain-name-servers row, and change the IP addresses to 10.0.2.10.
8. When satisfied with the data, click Import.
    You can view the status of the importation process and a summary report in the Data Import Wizard Log.
9. To enable DDNS updates, log in to the Grid Master, from the Data Management tab, select the DHCP tab, expand the Toolbar and click Grid DHCP Properties.
10. In the DDNS -> Basic tab of the Grid DHCP Properties editor, select Enable DDNS Updates.
11. Save the configuration and click Restart if it appears at the top of the screen.
12. To check the imported DHCP configuration file, from the Data Management tab, select the DHCP tab -> Members tab -> 10.0.2.10 -check box. Expand the Toolbar and click View DHCP Configuration.
13. In the DHCP configuration file, check that all the imported subnets are present, and navigate to the beginning of the file and check that you see the \texttt{ddns-updates on} statement. (If you see \texttt{ddns-updates off}, enable DDNS updates for the Grid as explained in steps 9-12.)

Importing DHCP Data for Site 1

1. Repeat the steps in Importing DHCP Data for HQ and Site 2, saving the DHCP configuration file from your legacy DHCP server at 10.1.1.20, and importing it to the Grid Master at 10.0.1.10 for the member with IP address 10.1.1.10 to serve.
2. Check the imported DHCP configuration file by logging in to the Grid Master and from the Data Management tab, select the DHCP tab -> Members tab -> 10.1.1.10 -check box. Expand the Toolbar and click View DHCP Configuration.

Importing DHCP Data for Site 3

1. Repeat the steps in Importing DHCP Data for HQ and Site 2, saving the DHCP configuration file from your legacy DHCP server at 10.1.1.20, and importing it to the Grid Master at 10.0.1.10 for the member with IP address 10.3.1.10 to serve.
2. After the importation process completes, check the imported DHCP configuration file by logging in to the Grid Master and from the Data Management tab, select the DHCP tab -> Members tab -> 10.3.1.10 -check box. Expand the Toolbar and click View DHCP Configuration.

Import DNS Data

Using the Infoblox Data Import Wizard, import DNS data from the legacy hidden primary server at 10.0.1.5 to the new hidden primary server at 10.0.1.10 (the Grid Master). There are three phases to this task:

- **Before Using the Wizard:**
  - Save the named.conf file from the legacy server to a file in a local directory on your management system.
  - Enable the legacy server to perform zone transfers to the NIOS appliance.
  - Configure three name server groups for the Grid, and allow the Grid Master/hidden primary DNS server at 10.0.1.10 to receive DDNS updates from the Grid members at 10.0.2.10, 10.1.1.10, and 10.3.1.10. These members act as secondary DNS servers and DHCP servers.
- **Using the Wizard:** Define the source, destination, and type of DNS data in the DNS configuration file (named.conf) that you want to import.
- **After Using the Wizard:** Check the imported DNS configuration file.

In this example, all the DNS data is in BIND 9 format. The Data Import Wizard supports various types of DNS formats, such as the following:

- BIND 4, 8, and 9
- Microsoft
- Lucent VitalQIP
- Nortel NetID
Before Using the Wizard
You must set up the legacy server and Grid Master before using the Data Import Wizard.

Legacy Server

1. Log in to the legacy name server at 10.0.1.5 and save the named.conf file, which contains all the DNS settings that you want to import into the Infoblox name server, to a local directory on your management system.
2. On the legacy server, enable zone transfers to the NIOS appliance.

Infoblox Grid Master – DDNS Updates

1. Log in to the Grid Master at 10.0.1.10, and from the Data Management tab, select the DNS tab -> Members tab -> 10.0.1.10 check box and select the Edit icon.
2. In the Member DNS Configuration editor, select the Updates tab -> Basic tab and enter the following:
   - Select Override.
   - Allow updates from: Click the Add icon and select IPv4 Address. Enter 10.0.2.10 in the Name field of the new row.
3. Click the Add icon again and add 10.1.1.10 and 10.2.1.10 as IP addresses from which you allow DDNS updates.
4. Save the configuration and click Restart if it appears at the top of the screen.

Note: When all DNS servers are members in the same Grid, the members use database replication to synchronize all their data—including DNS zone data. You can change the default behavior so that Grid members use zone transfers instead. In this example, Grid members use database replication.

Infoblox Grid Master – Name Server Groups

1. From the Data Management tab, select the DNS tab -> Name Server Groups tab.
2. Click the Add icon to open the Add Name Server Group wizard.
3. Enter the following:
   - Name Server Group Name: HQ-Group
4. Click the Add icon and add the following:
   - Grid Primary: ns1.corpxyz.com; Stealth: Select this check box.
   - Grid Secondary: ns2.corpxyz.com; Grid replication (recommended): Select this check box.
5. Click Save & New.
6. Repeat steps 2 to 4 to create another group. Name it Site1-Group, and use ns1.corpxyz.com as the hidden primary server, ns3.corpxyz.com as a secondary server, and Grid replication for zone updates.
7. Repeat steps 2 to 4 to create another group. Name it Site2-Group, and use ns1.corpxyz.com as the hidden primary server, ns4.corpxyz.com as a secondary server, and Grid replication for zone updates.

Using the Wizard

While progressing through the Data Import Wizard, you must define the source, destination, and type of DNS data that you want to import. You then make some simple modifications to the data and import it.

Defining the Source, Destination, and Type of DNS Data

1. Launch the Data Import Wizard.
2. After reading the information in the left panel of the welcome page, click Next.
3. Select Import to Infoblox Appliance, enter the following, and then click Next:
   - Hostname or IP address: 10.0.1.10
   - Username: admin
   - Password: 1n85w2IF
   - The Data Import Wizard Log opens in a separate window behind the wizard. Leave it open while you continue.
4. Select the following, and then click Next:
   - What kind of data would you like to import? DNS
   - Which legacy system are you importing from? BIND 9
   - Which appliance will be serving this data? 10.0.1.10
5. Select the following, and then click Next:
   - What BIND 9 DNS configuration file would you like to use? Click Browse, navigate to the named.conf file you saved from the legacy server, select it, and then click Open.
   - What type of BIND 9 DNS data do you want to import? DNS zone information and DNS record data
   - Where is the BIND 9 DNS record data? Zone transfer(s) from a DNS server; 10.0.1.5

The wizard displays two tables of data. The upper table contains global DNS server configuration parameters. The lower table contains zone
configurations.

The Data Import Wizard Log presents a summary listing the number of views, zones, and DNS records in the configuration file.

**Note:** Only superusers can import A, AAAA, shared A, and shared AAAA records with a blank name. Limited-access users must have read/write permission to adding a blank A/AAAA record in order to import A, AAAA, shared A, and shared AAAA records with a blank name, otherwise the import operation might fail. You can assign global permission for specific admin groups and roles to allow to import A, AAAA, shared A, and shared AAAA records with a blank name. For more information, see Administrative Permissions for Adding Blank A or AAAA Records.

### Modifying DNS Data

While importing data from the legacy DNS server, you cancel the importation of global configuration settings, and apply the name server groups you created in Before Using the Wizard to the zones you want to import.

1. In the Global DNS Configuration table, select all rows by clicking the top row and then SHIFT+clicking the bottom row.
2. Right-click the selected rows to display the Set Import Options dialog box, select Do not import, and then click Apply.
3. In the DNS Zones table, clear the Import check box for the default view.
4. Select corpxyz.com, lab.corpxyz.com and all the corresponding reverse-mapping zones.
5. Right-click the selected rows, and then select Set Import Options.
6. In the Set Import Options dialog box, enter the following, and then click Apply:
   - Set Zone Type: No change
   - Set Import Option: No change
   - Set View: default
   - Set Member: HQ-Group master
7. Select site1.corpxyz.com and all the reverse-mapping zones with 1 in the second octet in the zone name (1.1.10.in-addr.arpa, 2.1.10.in-addr.arpa, 3.1.10.in-addr.arpa, and so on).
8. Right-click the selected rows, and select Set Import Options.
9. In the Set Import Options dialog box, make the same selections as in 6, but choose Site1-Group master from the Set Member drop-down list.
10. Similarly, select site2.corpxyz.com and all the reverse-mapping zones with 2 in the second octet in the zone name.
11. Right-click the selected rows, and select Set Import Options.
12. In the Set Import Options dialog box, make the same selections as in 6, but choose Site2-Group master from the Set Member drop-down list.

### Importing DNS Data

1. Click Import.
   - The wizard imports the global DNS parameters and zone-specific configuration settings from the named.conf file and performs a zone transfer of the data from the legacy server.
2. Use the Data Import Wizard Log to monitor progress and review results afterward.
   - The log lists all the zones that the wizard imports and concludes with a total of all the successfully and unsuccessfully imported zones.
   - **Note:** If the wizard is unable to import a zone, an error message with an explanation appears in the log.
3. To close the Data Import Wizard, click Exit. This closes the Data Import Wizard Log as well.

### After Using the Wizard

After you import data, you must restart services on the Grid Master and delete the A records for the legacy servers from the corpxyz.com zone. You can also confirm that the imported data is correct and complete by checking the DNS configuration and the forward- and reverse-mapping zones.

1. Log in to the Grid Master (10.0.1.10), select the Grid tab, expand the Toolbar, and then click the Restart Services icon.
   - **Note:** When importing data through the wizard rather than entering it through the GUI, the Restart Services icon does not change to indicate you must restart service for the appliance to apply the new data. Still, restarting service on the Grid Master is necessary for the imported configuration and data to take effect.
2. To remove A records for the legacy servers, from the Data Management tab, select DNS tab -> Zones tab -> corpxyz.com.
3. Expand the Records section, select the following A records in the corpxyz.com zone, and then click the Delete icon:
   a. ns1 (for 10.0.1.5)
   b. ns2 (for 10.0.2.5)
   c. ns3.site1.corpxyz (for 10.1.1.5)
   d. ns4.site3.corpxyz (for 10.2.1.5)
4. Remove the respective A records for legacy servers from the site1.corpxyz and site3.corpxyz subzones.
5. To check the imported DNS configuration file, from the Data Management tab, select DNS tab -> Members tab 10.0.1.10 check box.
   - Expand the Toolbar and click View -> View DNS Configuration.
If you do not see the imported DNS configuration file, make sure you enabled DNS and restarted services.

Scroll through the DNS configuration log to check that each imported zone has an allow-update statement like the following one for the 10.1.10.in-addr.arpa reverse-mapping zone:

```plaintext
zone "10.1.10.in-addr.arpa" in {
    ...
    allow-update { key DHCP_UPDATER; 10.0.2.10; 10.1.1.10; 10.2.1.10; };
    ...
};
```

Enable DHCP and Switch Service to the Grid

Finally, you must enable DHCP service on the three Grid members at 10.0.2.10, 10.1.1.10, and 10.2.1.10, and switch DNS and DHCP service from the legacy DNS and DHCP servers to them.

1. Log in to the Grid Master (10.0.1.10) and from the Data Management tab, select the DHCP tab -> Members tab -> 10.0.2.10 check box. Expand the Toolbar and click Start.
2. Repeat step 1 to enable DHCP on 10.1.1.10 and 10.3.1.10.

Note: Start the DNS service, as described in Starting and Stopping the DNS Service. The Grid members are ready to serve DHCP and DNS, and send DDNS updates.

Managing a Grid

After you configure a Grid Master and add members, you might need to perform the following tasks:

- Changing Grid Properties
- Configuring Security Level Banner
- Configuring Notice and Consent Banner
- Configuring Informational Level Banner
- Setting the MTU for VPN Tunnels
- Removing a Grid Member
- Promoting a Master Candidate

Changing Grid Properties

You can change a Grid name, its shared secret, and the port number of the VPN tunnels that the Grid uses for communications. Note that changing the VPN port number, time zone, date or time requires a product restart.

To modify the properties of a Grid:

1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and select Grid Properties -> Edit.
3. In the Grid Properties editor, select the General tab -> click the Basic tab, and then modify any of the following:

   - **Grid Name**: Type the name of a Grid. The default name is Infoblox.
   - **Shared Secret**: Type a shared secret that all Grid members use to authenticate themselves when joining the Grid. The default shared secret is test.
   - **Shared Secret Retype**: Type the shared secret again to confirm its accuracy.
   - **Time Zone**: Choose the applicable time zone from the drop-down list.
   - **Date**: Click the calendar icon to select a date or enter the date in YYYY/MM/DD format.
   - **Time**: Click the clock icon to select a time or enter the time in HH:MM:SS format.
   - **VPN Port**: Type the port number that the Grid members use when communicating with the Grid Master through encrypted VPN tunnels. The default port number is 1194. For more information, see Port Numbers for Grid Communication.
   - **Enable Recycle Bin**: Select the check box to enable the Recycle Bin. The Recycle Bin stores deleted items when the user deletes Grid, DNS, or DHCP configuration items. Enabling the Recycle Bin allows you to undo deletions and to restore the items on the appliance at a later time. If you do not enable this feature, deleted items from the GUI are permanently removed from the database.
   - **Audit Logging**: Select one of the following:
     - **Detailed**: This is the default type. It is automatically selected. It provides detailed information on all administrative changes such as the date and time stamp of the change, administrator name, changed object name, and the new values of all properties.
     - **Brief**: Provides information on administrative changes such as the date and time stamp of the change, administrator name, and the changed object name. It does not show the new value of the object.
   - In the Grid Properties editor, select the General tab -> click the Advanced tab (or click Toggle Advanced Mode) and modify any of the following:
     - **Enable GUI Redirect from Member**: Select this check box to allow the appliance to redirect the Infoblox GUI from a
Grid member to the Grid Master.

**Note:** If read-only API access is enabled for a Grid Master Candidate, then selecting the Enable GUI Redirect from Member check box for the Grid Master Candidate does not redirect the Infoblox GUI from the Grid Master Candidate to the Grid Master. For more information about enabling read-only API access on a Grid Master Candidate, see Enabling Read-only API Access on the Grid Master Candidate.

- **Enable GUI/API Access via both MGMT and LAN1/VIP:** Select this check box to allow access to the Infoblox GUI and API using both the MGMT and LAN1 ports for standalone appliances and MGMT and VIP ports for an HA pair. This feature is valid only if you have enabled the MGMT port. For information about enabling the MGMT port, see Appliance Management.

**Note:** The appliance uses the MGMT port only to redirect the Infoblox GUI from a Grid member to the Grid Master even after you enable the Enable GUI/API Access via both MGMT and LAN1/VIP feature.

- **Show Restart Banner:** Select this check box to enable the appliance to display the Restart Banner at the top of Grid Manager whenever the appliance notifies you that a service restart is required.
- **Require Name:** Select this check box to prompt the administrator to input the user name before performing the service restart. When you select this check box, the appliance displays the Confirm Restart Services dialog box. Enter the user name in the Name field and click Restart Services. For information about restarting service, see Restarting Services.

4. Save the configuration.

If you changed the VPN port number, time zone, date or time, Grid Manager displays a warning indicating that a product restart is required. Click Yes to continue, and then log back in to Grid Manager after the application restarts.

### Configuring Security Level Banner

You can publish a security banner that indicates the security level of the Infoblox Grid. It appears on the header and footer of all pages of Grid Manager. The security level can be Top Secret, Secret, Confidential, Restricted, and Unclassified. Each message type is associated with a predefined security level color. You can modify this color at any point of time. Grid Manager automatically uses an appropriate contrasting text font color that goes with the banner color. Only superusers can configure and enable this feature.

To configure the advanced security level banner for a Grid:

1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and select Grid Properties -> Edit.
3. In the Grid Properties editor, select the Security tab -> Advanced tab.
4. Complete the following:
   - **Enable Security Banner:** Select this to enable the display of the security banner.
   - **Security Level:** From the drop-down list, select the security level for the banner.
   - **Security Level Color:** The default color is displayed in the drop-down. If necessary using the drop-down list, select the required color for the security level banner. When you change the security level, Grid Manager resets default color for that level.
   - **Classification Message:** Enter the message you want to display in the security banner. You can enter up to 190 characters.
5. Save the configuration.

Security banner appears on the header and footer of the Grid Manager screen including the Login screen.

### Configuring Notice and Consent Banner

You can configure and publish a notice and consent banner as the first login screen that includes specific terms and conditions you want end users to accept before they log in to the Infoblox Grid. When an end user tries to access Grid Manager, this banner is displayed as the first screen. The user must accept the terms and conditions displayed on the consent screen before accessing the login screen of Grid Manager. Only superusers can configure and enable this feature.

To configure the notice and consent banner:

1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and select Grid Properties -> Edit.
3. In the Grid Properties editor, select the Security tab -> Advanced tab, and then complete the following:
   - **Enable Notice and Consent Banner:** Select the check box to enable the display of the notice and consent banner. In the text field, enter the message that you want to be included in the banner. The message cannot exceed 10,000 characters.
4. Save the configuration.

This banner appears as the first screen when users access Grid Manager. Users must read the terms and conditions and then click Accept on the consent screen before they can access the login screen of Grid Manager.

### Configuring Informational Level Banner

You can publish the informational banner for multiple uses, such as to indicate whether the Infoblox Grid is in production or a lab system. The banner can also be used for issuing messages of the day. The informational level banner appears on the header of the Grid Manager screen. You can publish the banner information you want and set the banner color. Grid Manager automatically uses an appropriate contrasting text font color.

Copyright ©2019, Infoblox, Inc. All right reserved.
that goes with the banner color. Only superusers can configure and enable this feature. To configure the advanced informational banner for a Grid:

1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and select Grid Properties -> Edit.
3. In the Grid Properties editor, select the General tab -> Advanced tab
4. Complete the following:
   - Enable informational GUI Banner: Select the check box to enable the display of the informational banner message.
   - Banner Color: The default color is displayed in the drop-down. If necessary using the drop-down list, select the required color for the informational level banner.
   - Message: Enter the message you want to display in the informational banner. You can enter up to 190 characters.
5. Save the configuration.

Informational banner appears on the header of the Grid Manager screen.

Configuring Recursive Deletions of Networks and Zones

Through Grid Manager, you can configure the group of users that are allowed to delete or schedule the deletion of a network container and its child objects as well as a zone and its child objects. For information about how to delete a network container or zone, see Deleting Network Containers and Removing Zones.

When you select All Users or Superusers, these users can choose to delete a parent object and re-parent its child objects, or they can choose to delete a parent object and all its child objects. These options appear only if a network container or a zone has child objects. For information about scheduling recursive deletion of network containers and zones, see Scheduling Recursive Deletions of Network Containers and Zones.

When you select Nobody, all the users can delete the parent object only. All the child objects, if any, are re-parented. For information about scheduling deletions, see Scheduling Deletions. Note that you can restrict specific users to perform recursive deletions of network containers and zones only through Grid Manager. These settings do not prevent other users from performing recursive deletions through the API.

Note: You must have Read/Write permission to all the child objects in order to delete a parent object. Recursive deletion is applicable to all zone types except stub and forward-mapping zones.

The appliance puts all deleted objects in the Recycle Bin, if enabled. You can restore the objects if necessary. When you restore a parent object from the Recycle Bin, all its contents, if any, are re-parented to the restored parent object. For information about the Recycle Bin, see Using the Recycle Bin.

To configure the group of users to perform recursive deletions:

1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and select Grid Properties -> Edit.
3. In the Grid Properties editor, select the General tab -> Advanced tab.
4. Under Present the option of recursive deletion of networks or zones to, select one of the following:
   - All Users: Select this to allow all users, including superusers and limited-access users, to choose whether they want to delete the parent object and its contents or the parent object only when they delete a network container/network or a zone. This is selected by default.
   - Superuser: Select this to allow only superusers to choose whether they want to delete the parent object and its contents or the parent object only when they delete a network container/network or a zone.
   - Nobody: When you select this, users can only delete the parent object (network container or zone). All child objects, if any, are re-parented.
5. Save the configuration.

Setting the MTU for VPN Tunnels

You can configure the VPN MTU (maximum transmission unit) for any appliance with a network link that does not support the default MTU size (1500 bytes) and that cannot join a Grid because of this limitation. If an appliance on such a link attempts to establish a VPN tunnel with a Grid Master to join a Grid, the appliance receives a PATH-MTU error, indicating that the path MTU discovery process has failed. For information about the MTU discovery process, see RFC 1191, Path MTU Discovery.

To avoid this problem, you can set a VPN MTU value on the Grid Master for any appliance that cannot link to it using a 1500-byte MTU. When the appliance contacts the master during the key exchange handshake that occurs during the Grid-joining operation, the master sends the appliance the MTU setting to use.

To set the VPN MTU for a Grid member:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box -> Edit icon.
2. Select the Network -> Advanced tab of the Grid Member Properties editor.
3. In the VPN MTU field, enter a value between 600 and 1500.
4. Save the configuration and click Restart if it appears at the top of the screen.

Removing a Grid Member

You might want or need to remove a member from a Grid, perhaps to disable it or to make it an independent appliance or an independent HA pair. Before you remove a member, make sure that it is not assigned to serve any zones or networks.
To remove a Grid member, from the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and click the Delete icon.

Promoting a Master Candidate

To promote a Master candidate to a Grid Master, you must have previously designated a Grid member as a Master Candidate. Select the Master Candidate option in the General tab of the Grid Member Properties editor to designate the member as a Master Candidate. You can designate any member as a Master Candidate. The Grid Master Candidate gets a complete copy of the Grid database. Therefore, Infoblox recommends that you configure the same appliance models for the Grid Master and Grid Master Candidates. By default, Grid Master promotion uses UDP port 1194. Make sure that UDP 2114 and UDP 1194 ports are open between the Grid members and newly designated Grid Master. During a Grid Master promotion, the newly-promoted Grid Master continuously contacts all Grid members, including the original Grid Master on UDP port 2114 until it reaches them. It notifies all Grid members that it is the new Grid Master. The Grid Members restart and then attempt to establish normal Grid communications (via BloxSync) with the newly promoted Grid Master. Before promoting a Master Candidate, check your firewall rules to ensure that the Master Candidate can communicate with all the Grid members. For information, see Grid Communications.

To promote a Master Candidate, you can make a direct serial connection to the console port on the active node of an HA Candidate or to the console port on a single Candidate. You can also make a remote serial connection (using SSH v2) to the candidate. Enter the following Infoblox CLI command to promote a Master Candidate:

```
set promote_master.
```

You can do one of the following to promote a Master Candidate:

- Immediately notify all Grid members about the promotion.
- Set a sequential notification to provide wait time for Grid members to join the new Grid Master. Staggering the restarts of Grid members can minimize DNS outages. The sequential order for Grid members to join the new Grid Master begins with the old Grid Master and then the Grid members in FQDN order. The default delay time is 120 seconds. You can configure the delay time from a minimum of 30 seconds up to 600 seconds.

**Note:** During a Grid Master promotion, ensure that you do not designate a Grid member as a Grid Master Candidate or promote a Master Candidate. In addition, wait up to two hours since the last promotion to perform another Grid Master promotion. Otherwise, you might experience unnecessary member reboots. Whenever possible, separate any operations that require product restarts by at least an hour.

To promote a Master Candidate, do the following:

1. **Establish a serial connection (through a serial console or remote access using SSH) to the Master Candidate.** For information about making a serial connection, see Method 2 – Using the CLI.
2. **At the CLI prompt, use the command set promote_master to promote the Master Candidate and send notifications to all Grid members immediately, or promote the Master Candidate to the Grid Master immediately and specify the delay time for the Grid members to join the new Grid Master.** For more information about the command, refer to the Infoblox CLI Guide.
3. **To verify the new master is operating properly, log in to the Infoblox Grid Manager on the new master using the VIP address for an HA master or the IP address of the LAN1 port for a single master.**
4. **Check the icons in the Status column.** Also, select the master, and then click the Detailed Status icon in the table toolbar. You can also check the status icons of the Grid members to verify that all Grid members have connected to the new master. If you have configured a delay time for Grid member notification, it will take some time for some members to connect to the new master. You can also check your firewall rules and log in to the CLI to investigate those members.

**Note:** Note that when you promote the Master Candidate to a Grid Master, the IP address will change accordingly. If you have configured a FireEye appliance, then any changes in the Grid Master IP address, FireEye zone name, associated network view or the DNS view will affect the Server URL that is generated for a FireEye appliance. The FireEye appliance will not be able to send alerts to the updated URL when there is a change in the IP address. You must update the URL in the FireEye appliance to send alerts to the NIOS appliance. For more information, see Configuring FireEye RPZs.

Enabling Read-only API Access on the Grid Master Candidate

You can enable read-only API access on the Grid Master Candidate to provide additional scalability of read/write API requests on the Grid Master, which in turn improves the performance of the Grid Master. The read-only API access is disabled by default for new installations. When you enable read-only API access on an HA Grid Master Candidate, you can access the API service only on the active node. If the API service is disabled for an admin group, the users in the admin group cannot access read-only API service on the Grid Master Candidate, even though read-only API access is enabled for the Grid Master Candidate. Also, the users in the admin group should have at least read-only permission to access the API service.

**Note:** When you upgrade the Grid Master Candidate to NIOS 7.1 and later, read-only API access is disabled. But when you upgrade the Grid Master Candidate from NIOS 7.1 to a later release with read-only API access enabled, then this setting is retained after the upgrade is completed.

The appliance logs all API logins in the audit log and syslog. You can view the audit log and syslog of the Grid Master Candidate under the Administration -> Logs tab.

To enable read-only API access on the Grid Master Candidate:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_Master_Candidate check box, and then click the Edit icon.
In the Grid Member Properties editor, select the General tab -> Basic tab, and then do the following:

**Read Only API access**: This field is displayed only when the Grid member is designated as a Master Candidate. Select this check box to enable read-only API access on the Grid Master Candidate. Enabling this check box will only allow read-only API access and not write API access. Note that if you enable this check box, you cannot access the GUI using the IP address of the Grid Master Candidate.

2. Save the configuration.

**About the Master Grid**

A Master Grid provides centralized management of multiple Grids. When a Grid is managed by a Master Grid, the Master Grid icon appears on the left side of the top panel of Multi-Grid Manager. Assuming you have permission, you can click this icon to access Multi-Grid Manager. In addition, the Toolbar provides several functions for joining the Master Grid, editing its properties and leaving the Master Grid. For more information about the Master Grid and these functions, refer to the Multi-Grid Manager Administrator Guide.

**Chapter 6 Deploying Independent Appliances**

This chapter explains how to deploy single independent appliances and independent HA pairs. Independent appliances run NIOS without the Grid upgrade and are deployed independently from a Grid. This chapter includes the following sections:

- Deploying a Single Independent Appliance
  - Method 1 – Using the LCD
  - Method 2 – Using the CLI
  - Method 3 – Using the Infoblox NIOS Startup Wizard
- Changing the Communication Protocol for a Dual Mode Independent Appliance
- Configuration Example: Deploying a NIOS Appliance as a Primary DNS Server
  - Cabling the Appliance to the Network and Turning On Power
  - Specifying Initial Network Settings
  - Specifying Appliance Settings
  - Enabling Zone Transfers on the Legacy Name Server
  - Importing Zone Data on an Independent Appliance
  - Designating the New Primary on the Secondary Name Server (at the ISP Site)
  - Configuring NAT and Policies on the Firewall
- Deploying an Independent HA Pair
  - Using the Infoblox NIOS Startup Wizard to Configure an HA Pair
- Configuration Example: Configuring an HA Pair for Internal DNS and DHCP Services
  - Cabling Appliances to the Network and Turning On Power
  - Specifying Initial Network Settings
  - Specifying Appliance Settings
  - Enabling Zone Transfers
  - Importing Zone Data
  - Defining Networks, Reverse-Mapping Zones, DHCP Ranges, and Infoblox Hosts
  - Defining Multiple Forwarders
  - Enabling Recursion on External DNS Servers
  - Modifying the Firewall and Router Configurations
  - Enabling DHCP and Switching Service to the NIOS Appliance
  - Managing and Monitoring
- Verifying the Deployment
  - Single Independent Appliance
  - Independent HA Pair
- Infoblox Tools for Migrating Bulk Data

**Independent Deployment Overview**

*Note*: Infoblox appliances support IPv4 and IPv6 networking configurations in most deployments cited in this chapter. You can set the LAN1 port to an IPv6 address and use that address to access the NIOS UI and the NIOS Setup Wizard. All HA operations can be applied across IPv6. You can also set a dual mode appliance by configuring both IPv4 and IPv6 address for the LAN1 port. Topics in this and following chapters generally use IPv4 examples. Also note that LAN2 and the MGMT port also support IPv6. DNS services are fully supported in IPv6 for the LAN1, LAN2, MGMT and VLAN ports. DHCP services are fully supported in IPv6 for the LAN1 and LAN2 ports. Example networks throughout this chapter use IPv4 addressing.

You can deploy the NIOS appliance as a Grid member in an Infoblox Grid or independently as a standalone deployment. NIOS appliances support both IPv4 and IPv6 networks and you can deploy them in either IPv4, IPv6, or dual mode (IPv4 and IPv6). Grids offer many advantages for large organizations while independent deployments can be sufficient for smaller sites. For example, if your ISP hosts one name server to respond to external DNS queries, you can deploy a single independent NIOS appliance as the other name server, as shown in 4823826.

*Figure 6.1 Single Independent Appliance as a DNS Server*
Using primary and secondary name servers provides DNS protocol redundancy, and configuring two DHCP servers as DHCP failover peers provides DHCP protocol redundancy. However, you can only have hardware redundancy if you deploy appliances in an HA (high availability) pair. Should the active node in an HA pair fail, the passive node becomes active and begins serving data, as shown in Figure 6.2. For more information about HA pairs, see About HA Pairs.

System Manager GUI
When you deploy an independent appliance, you use System Manager to manage the appliance. Though other chapters in this guide contain information that assumes a Grid deployment and describes the Grid Manager GUI, most of the configuration procedures are applicable to an independent appliance, with the following differences:

- In the Dashboard, there is no Grid Status widget, and the Members Status widget in Grid Manager is the System Status widget in System Manager.
- Functions related to a Grid, such as joining a Grid and managing Grid licenses, do not exist in System Manager.
- The Grid related tabs and functions in Grid Manager are the system related tabs and functions in System Manager.
- Functions related to the Members tab in Grid Manager appear in the Nodes tab or the Toolbar of another subtab in System Manager.

For example, the following navigation path for a Grid:

- From the Grid tab, select the Grid Manager tab -> Members tab -> member check box, and then click HTTPS Cert -> Download Certificate from the Toolbar.

is the following for an independent appliance:
Deploying a Single Independent Appliance

To deploy a single independent NIOS appliance, you cable its LAN1 port to the network and change its default IP settings so that it can connect to its surrounding IP address space. The default LAN settings are as follows:

- IP address: 192.168.1.2
- Netmask: 255.255.255.0
- Gateway: 192.168.1.1

When deploying a single independent appliance, you can use one of the following methods to set up the initial configuration:

- **Method 1 - Using the LCD**
  - Requirements: Physical access to a powered up NIOS appliance.
  - Advantage: You do not need any other equipment.

- **Method 2 - Using the CLI**
  - Requirements: A serial connection from your management system to the console port on the NIOS appliance. You can also enable remote console access so that you can use the CLI over a network connection. For information, see Restricting GUI/API Access.
  - Advantage: You do not need to change the IP address of the management system to connect to the NIOS appliance.

- **Method 3 - Using the Infoblox NIOS Startup Wizard**
  - Requirements: An HTTPS connection from your management system to the LAN1 port on the NIOS appliance.
  - Advantage: The wizard provides step-by-step guidance for changing not only the IP settings for the LAN1 port, but also changing the appliance host name and admin password, setting the system clock, and—if using NTP (Network Time Protocol)—enabling the NIOS appliance to be an NTP client.

Note that you can configure network settings using the Startup wizard any time after you have configured the appliance. To start the wizard, from System Manager, select the System tab, and then click System Properties -> Startup Wizard from the Toolbar.

After you configure the network settings on a single independent appliance, you can migrate data from legacy DNS and DHCP servers to the NIOS appliance. Several tools and methods are available for migrating data and configuration settings. For a list of the available options, see InfoBlox Tools for Migrating Bulk Data.

**Method 1 – Using the LCD**

Some of the NIOS appliances have an LCD and navigation buttons on the front panel that allow you to view system status and license information as well as configure network settings for the LAN1 port.

*Figure 6.3 Infoblox LCD and Navigation Buttons*

You can deploy a single independent NIOS appliance by setting its LAN1 port IP address, netmask, and gateway through the LCD. This is the simplest method because you do not need anything other than a physical access to the appliance to complete the initial configuration.

*Note:* LCD does not support IPv6 addressing.

1. Connect the power cable from the NIOS appliance to a power source and turn on the power.
   At startup, the Infoblox logo appears in the LCD on the front panel of the appliance. Then the LCD scrolls repeatedly through a series of display screens.
2. To change the network settings for the LAN1 port, press one of the navigation buttons.
   The LCD immediately goes into the input mode, in which you can enter the IP address, netmask, and gateway for the LAN1 port.
3. Use the navigation buttons to enter an IP address, netmask, and gateway address for the LAN1 port.
4. Cable the LAN1 port of the NIOS appliance to a network as described in the installation guide that shipped with your product.

**Method 2 – Using the CLI**

You can use the Infoblox CLI to make an initial network configuration through the set network command. To access the CLI, make a direct serial connection from your management system.

1. Connect a console cable from the console port on your workstation to the male DB-9 console port on the NIOS appliance. The DB-9 pin assignments follow the EIA232 standard. You can use one RJ-45 rollover cable and two female RJ-45-to-female DB-9 adapters, or a female DB-9-to-female DB-9 null modem cable.

*Figure 6.4 Console Connection*
2. Use a serial terminal emulation program, such as Hilgraeve Hyperterminal® (provided with Windows® operating systems), to launch a session. The connection settings are:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Xon/Xoff

3. Log in to the appliance using the default username and password (admin and infoblox).

4. At the Infoblox command prompt, enter `set network` to change the network settings, such as the IP address, netmask, and gateway for the LAN1 port. You can configure either IPv4 or IPv6 address for the LAN1 port.

   **Note:** In the following example, the variable `ip_addr1` is the IP address of the LAN1 port and `ip_addr2` is the IP address of the gateway for the subnet on which you set the `ip_addr1` address. Infoblox appliances support IPv4 and IPv6 networking configurations in all deployments cited in this chapter. You can set the LAN1 port to an IPv6 address and use that address to access the NIOS UI.

You can configure an IPv4 address for the LAN1 port as follows:

```
Infoblox > set network
NOTICE: All HA configuration is performed from the GUI. This interface is used only to configure a standalone node or to join a Grid.
Enter IP address: ip_addr1
Enter netmask: netmask
Enter gateway address: ip_addr2
Configure IPv4 network settings? (y or n): y
Enter IPv4 address [Default: none]: 2001:db8:a22:a00::29
Enter IPv4 Prefix Length [Default: none]: 64
Enter IPv4 gateway [Default: none] 2001:db8:a22:a00::1
Become Grid member? (y or n): n
```

To avoid configuring IPv6 network settings, you can press N at the command line.

You can configure an IPv6 address for the LAN1 port as follows:

```
Infoblox > set network
NOTICE: All HA configuration is performed from the GUI. This interface is used only to configure a standalone node or to join a grid.
Enter IP address : 2620:010A:6000:2400:0000:0000:0000:6508
Enter IPv6 Prefix Length: 64
Enter IPv6 gateway [Default: none]: 2620:010A:6000:2400:0000:0000:0000:0001
Configure IPv4 network settings? (y or n):n
```
Become grid member? (y or n): n

To configure IPv4 network settings, you can press Y at the command line and configure IPv4 address, netmask, and the gateway address. After you confirm your network settings, the Infoblox application automatically restarts. You can press N to avoid configuring IPv6 on the command line. After you confirm your network settings, the Infoblox application automatically restarts.

5. Cable the LAN1 port to a network. For information about installing and cabling the appliance, refer to the user guide or installation guide that was shipped with the product.

Method 3 – Using the Infoblox NIOS Startup Wizard

When you first make an HTTPS connection to a NIOS appliance, the Infoblox NIOS Startup Wizard guides you through the deployment options and basic network settings. You can also change the password of the superuser (admin) and set up the system clock.

Note that you can configure network settings using the Startup wizard any time after you have configured the appliance. To start the wizard, from Grid Manager, select the System tab, and then click System Properties -> Startup Wizard from the Toolbar.

To make an HTTPS session to the appliance, you must be able to reach its IP address from the management system.

Note: If you have already set the IP address of the LAN1 port through the LCD or CLI so that you can reach it over the network—and you have already cabled the appliance to the network—you can skip the first step.

1. If you have not changed the default IP address (192.168.1.2/24) of the LAN1 port through the LCD or CLI—and the subnet to which you connect the appliance is not 192.168.1.0/24—put your management system in the 192.168.1.0/24 subnet and connect an Ethernet cable between the management system and the appliance.

2. Open an Internet browser window and enter https://<IP address of the appliance> to make an HTTPS connection. For information about supported browsers, see Supported Browsers.

Several certificate warnings may appear during the login process because the preloaded certificate is self-signed and has the hostname www.infoblox.com, which may not match the destination IP address you entered in step 1. To stop the warning messages from occurring each time you log in, you can disable certificate checks by entering the following command:

    set aclconfig verify_cert off

3. Enter your Infoblox username and password (admin and infoblox) on the Grid Manager login page, and then click Login or press Enter. For information, see Logging in to the GUI.

4. Read the Infoblox End-User License Agreement. If you want to participate in the Infoblox Customer Experience Improvement Program, complete the following:

   - Participate in the Infoblox Customer Experience Improvement Program: Select the check box to send product usage data to Infoblox on a periodic basis. Infoblox uses this data to improve product functionality. For more information about the program, see Participating in the Customer Experience Improvement Program.
   - Support ID (optional): Enter the Infoblox Support ID that was assigned to your account. It must be a number with four to six digits. The value you enter is also displayed in the Customer Improvement tab in the Grid Properties editor. Infoblox includes this ID in the data report.
   - Infoblox Privacy Policy: Click here to view the Infoblox privacy policy. The appliance displays the policy in a new browser tab. Click I Accept. The NIOS Setup wizard appears.

5. In the first screen of the NIOS Setup wizard, complete the following:

   - Type of Network Connectivity: Select the type of network connectivity for the appliance from the drop-down list:
     - IPv4 and IPv6: Select this to configure a dual mode appliance.
     - IPv4: Select this to configure an IPv4 appliance.
     - IPv6: Select this to configure an IPv6 appliance.

   - Are you configuring an HA pair or a standalone appliance?: Select Configuring a standalone appliance. To configure an independent HA pair, see Deploying an Independent HA Pair.

6. Click Next and complete the following to configure network settings:

   - Host Name: Enter a valid domain name for the appliance.
   - Ports and Addresses: This table lists the network interfaces based on the type of network connectivity of the appliance. For an IPv4 appliance, specify the network information for LAN1 (IPv4) interface and for an IPv6 appliance, specify the network information for LAN1 (IPv6) interface. For a dual mode appliance, specify the network information for both LAN1 (IPv4) and LAN1 (IPv6) interfaces.

   Enter correct information for the following by clicking the field:

   - Interface: Displays the name of the interface. You cannot modify this.
   - IP Address: Type the IPv4 or IPv6 address depending on the type of interface. An IPv6 address is a 128-bit number in colon hexadecimal notation. It consists of eight 16-bit groups of hexadecimal digits separated by colons (example: 2001:db8:0000:0123:4567:89ab:0000:cdef or 2001:db8::123:4567:89ab:0:cdef).
   - Subnet Mask (IPv4) or Prefix Length (IPv6): Specify an appropriate subnet mask for IPv4 address or prefix length for IPv6 address. The prefix length ranges from 2 to 127.
   - Gateway: Type the IPv4 or IPv6 address of the default gateway depending on the type of interface. For IPv6 interface, you can also type Automatic to enable the appliance to acquire the IPv6 address of the default gateway and the link MTU from router advertisements.
   - Port Settings: Select the port settings from the drop-down list. The list contains all the settings supported by the hardware model. The default is Automatic. The appliance automatically detects the port settings.

7. Click Next and complete the following to set admin password:

   - Yes: To change the default password.
**To keep the default password. Infoblox recommends that you change the default password.**
When you select Yes, complete the following:

- **Password**: Enter a password for the superuser admin account. The password must be a single alphanumeric string without spaces and at least four characters long. The password is case-sensitive.
- **Retype Password**: Enter the same password.

8. Click **Next** and complete the following to configure time settings:

- **Time Zone**: Select the applicable time zone from the drop-down list. The default is *(UTC)* Coordinated Universal Time.
- **Would you like to enable NTP?**: Select **Yes** to synchronize the time with external NTP servers, and then click the Add icon. Grid Manager adds a row to the NTP Server table. Click the row and enter either the IP address (IPv4 or IPv6) or the resolvable host name of an NTP server. You can view a list of public NTP servers at ntp.isc.org.
- **Select No** to specify the time settings for the appliance.
- **Date**: Enter the date in YYYY-MM-DD format. You can also click the calendar icon to select a date from the calendar widget.
- **Time**: Enter the time in HH:MM:SS AM/PM format. You can also click the clock icon to select a time from the drop-down list.

9. If you want to participate in the Infoblox Customer Experience Improvement Program, complete the following and then click **Next**:

- **Participate in the Infoblox Customer Experience Improvement Program**: Select the check box to send product usage data to Infoblox on a periodic basis. Infoblox uses this data to improve product functionality. For more information about the program, see *Participating in the Customer Experience Improvement Program*.
- **Support ID (optional)**: Enter the Infoblox Support ID that was assigned to your account. It must be a number with four to six digits. The value you enter here is also displayed in the *Customer Improvement* tab in the Grid Properties editor. Infoblox includes this ID in the data report.
- **Email**: Enter an email address to which Infoblox sends a copy of the usage report. The email address you enter here is also displayed in the *Customer Improvement* tab in the Grid Properties editor. This is optional.
- **Infoblox Privacy Policy**: Click here to view the Infoblox privacy policy. The appliance displays the policy in a new browser tab.

10. Click **Next** to view the summary of the configuration. Review the information and verify that it is correct. You can change the information you entered by clicking **Previous** to go back to a previous step.

11. Click **Finish**.
The appliance restarts and disconnects Grid Manager.

In a dual mode independent appliance, the communication protocol for all the services is set to IPv4, by default. You can change the default communication protocol for the services. For information, see *Changing the Communication Protocol for a Dual Mode Independent Appliance*.

### Changing the Communication Protocol for a Dual Mode Independent Appliance

You can change the default communication protocol for a dual mode appliance. You can force the appliance to use a specific protocol for the reporting services and for services with two types of resolution (A and AAAA records), you can set the preferred communication protocol.

To change the communication protocol for a dual mode independent appliance:

1. From the **System** tab, select the **System Manager** tab -> click **System Properties** from the Toolbar, and select **Edit** from the drop-down list.
2. In the **System Properties** editor, select the **Network** tab -> **Basic** tab, and then complete the following:

   - **Communication Protocol Settings and Preferences**: Select either IPv4 or IPv6 from the drop-down list. This setting will force the appliance to use the specified protocol for the reporting services and this is the preferred protocol for services with two types of resolution (A and AAAA records).
   - **Customized Settings**: Select this and do the following:
     - **Always use this Communications Protocol for**: Select either IPv4 or IPv6 from the drop-down list. This setting will force the appliance to use the specified communication protocol for reporting services.
     - **Always prefer this Communications Protocol for**: Select either IPv4 or IPv6 from the drop-down list to specify the preferred communication protocol for the listed services which has two types of resolution (A and AAAA records). The appliance uses the preferred protocol first for the service.

### Configuration Example: Deploying a NIOS Appliance as a Primary DNS Server

In this example, you configure the NIOS appliance as a primary DNS server for corpxyz.com. Its FQDN (fully-qualified domain name) is ns1.corpxyz.com. The interface IP address of the LAN1 port is 10.1.5.24. Because this is a private IP address, you must also configure the firewall to perform NAT (network address translation), mapping the public IP address 1.1.1.2 to 10.1.5.2. Using its public IP address, ns1 can communicate with appliances on the public network.

The FQDN and IP address of the external secondary DNS server are ns2.corpxyz.com and 2.2.2.2. The ISP hosts this server. You can deploy NIOS appliance in IPv4, IPv6, or dual mode (IPv4 and IPv6), but the configuration example uses IPv4 addresses.

The primary and secondary servers answer queries for the following public-facing servers in the DMZ:

- www.corpxyz.com
- mail.corpxyz.com
- ftp.corpxyz.com

When you create the corpxyz.com zone on the NIOS appliance, you import zone data from the legacy DNS server at 10.1.5.3.

*Figure 6.5 Example 1 Network Diagram*
Cabling the Appliance to the Network and Turning On Power
Connect an Ethernet cable from the LAN1 port of the NIOS appliance to a switch in the DMZ network and turn on the power. For information about installing and cabling the appliance, refer to the user guide or installation guide that ships with the product.

Specifying Initial Network Settings
Before you can configure the NIOS appliance through Grid Manager, you must be able to make a network connection to it. The default network settings of the LAN1 port are 192.168.1.2/24 with a gateway at 192.168.1.1 (the HA and MGMT ports do not have default network settings). To change these settings to suit your network, use either the LCD or the console port.

In this example, you change the IP address/netmask of the LAN1 port to 10.1.5.2/24, and the gateway to 10.1.5.1.

LCD
The NIOS appliance has an LCD and navigation buttons on its front panel.
At startup, the Infoblox logo appears in the LCD on the front panel of the appliance. Then the LCD scrolls repeatedly through a series of display screens.

1. To change the network settings from the default, press one of the navigation buttons.
   The LCD immediately goes into input mode, in which you can enter the IP address, netmask, and gateway for the LAN1 port.
2. Use the navigation buttons to enter the following information:
   - IP Address: 10.1.5.2
   - Netmask: 255.255.255.0
   - Gateway: 10.1.5.1

Specifying Appliance Settings
When you make the initial HTTPS connection to the NIOS appliance, the NIOS Startup Wizard guides you through the basic deployment of the appliance on your network. Use the wizard to enter the following information:

- Deployment: single independent appliance
- Host name: ns1.corpxyz.com
- Password: SnD34n534
- NTP (Network Time Protocol) server: 10.120.3.10; time zone: (UMT – 8:00 Pacific Time (US and Canada), Tijuana

1. Open an Internet browser window and enter https://10.1.5.2.
2. Accept the certificate when prompted.
   Several certificate warnings may appear during the login process. This is normal because the preloaded certificate is self-signed and has
the hostname www.infoblox.com, which does not match the destination IP address you entered in step 1. To stop the warning messages from occurring each time you log in to Grid Manager, you can generate a new self-signed certificate or import a third-party certificate with a common name that matches the FQDN (fully-qualified domain name) of the appliance. This is a very simple process. For information about certificates, see Creating a Login Banner.

3. Enter the default username and password (admin and infoblox) on the Grid Manager login page, and then click Login or press Enter. For information, see Logging in to the GUI.

4. Read the Infoblox End-User License Agreement, and then click I Accept to proceed. Grid Manager may take a few seconds to load your user profile.

5. In the first screen of the NIOS Startup wizard, complete the following:

- **Type of Network Connectivity**: Select IPv4 from the drop-down list.
- **Are you configuring an HA pair or a standalone appliance?**: Select Configuring a standalone appliance. To configure an independent HA pair, see Deploying an Independent HA Pair.

6. Click Next and complete the following to configure network settings:

- **Host Name**: Enter ns1.corpxyz.com.
- **Ports and Addresses**: Specify the network settings for LAN1(IPv4) port. Enter correct information for the following by clicking the field:
  - **IP Address**: Enter 10.1.5.2 as the IPv4 address for the LAN1 port.
  - **Subnet Mask (IPv4) or Prefix Length (IPv6)**: Enter 255.255.255.0 as the subnet mask for the LAN1(IPv4) port.
  - **Gateway**: Enter 10.1.5.1 as the gateway of the subnet on which the LAN1 port is set.
- **Port Settings**: Use the default value Automatic.

7. Click Next and complete the following to set admin password:

- **Would you like to set admin password?**: Click Yes.
- **Password**: Enter SnD34n534.
- **Retype Password**: Enter SnD34n534 again.

8. Click Next and complete the following to configure the time settings:

- **Time Zone**: Select UMT – 8:00 Pacific Time (US and Canada), Tijuana from the drop-down list.
- **Would you like to enable NTP?**: Select Yes to synchronize the time with external NTP servers, and then click the Add icon. Grid Manager adds a row to the NTP Server table. Click the row and enter 10.120.3.10 in the NTP Server field.

9. Click Next to view the summary of the configuration. Review the information and verify that it is correct. You can change the information you entered by clicking Previous to go back to a previous step.

10. Click Finish.

### Enabling Zone Transfers on the Legacy Name Server

To allow the appliance to import zone data from the legacy server 10.1.5.3, you must configure the legacy server to allow zone transfers to the appliance at 10.1.5.2.

#### Legacy BIND Server

- a. Open the named.conf file using a text editor and change the allow-transfer statement as shown below:

  **For All Zones** — To set the allow-transfer statement as a global statement in the named.conf file for all zones:

  ```
  options {
    zone-statistics yes;
    directory "/var/named/named_conf"; version "";
    recursion yes;
    listen-on { 127.0.0.1; 10.1.5.3; };
    ...
    allow-transfer {10.1.5.2 .}; transfer-format many-answers;
  }
  
  For a Single Zone — To set the allow-transfer statement in the named.conf file for the corpxyz.com zone:

  ```zone "corpxyz.com" in { type master;
    allow-transfer {10.1.5.2 .};
    notify yes;
  };
  ```

  2. After editing the named.conf file, restart DNS service on the appliance for the change to take effect.

#### Legacy Windows 2000/2003 Server

1. Click Start -> All Programs -> Administrative Tools -> DNS.
2. Click + (for ns1) -> + (for Forward Lookup Zones) -> corpxyz.com.
3. Right-click corpxyz.com, and then select Properties -> Zone Transfers.
4. On the Zone Transfers page in the corpxyz.com Properties dialog box, enter the following:

- **Allow zone transfers**: Select this.
- **Only to the following servers**: Select this.
Importing Zone Data on an Independent Appliance

You can import zone data from a legacy server or manually enter it. When you import both forward-mapping and reverse-mapping zone data, the NIOS appliance automatically creates Infoblox host records if corresponding A and PTR records are present. You can then modify the host records to add MAC addresses. However, if you only import forward-mapping zone data, the NIOS appliance cannot create host records from just the A records. In that case, because you cannot later convert A records to host records, it is more efficient to create the corpxyz.com zone, and define host records manually.

Infoblox host records are data models that represent IP devices within the Infoblox semantic database. The NIOS appliance uses a host object to define A, PTR, and CNAME resource records in a single object as well as a DHCP fixed address if you include a MAC address in the host object definition. The host object prevents costly errors because you only maintain a single object for multiple DNS records and a DHCP fixed address. Therefore, it is advantageous to use host records instead of separate A, PTR, and CNAME records.

**Note:** If you only have forward-mapping zones on your legacy servers and you want to add reverse-mapping zones and automatically convert A records to host records in the imported forward-mapping zones and create reverse host records in corresponding reverse-mapping zones, create the reverse-mapping zones on the NIOS appliance and then import the forward-mapping zones data. The NIOS appliance automatically converts the imported A records to host records in the forward-mapping zones and creates reverse host records in the reverse-mapping zones.

You also have the option of using the Data Import Wizard for loading DNS and DHCP data. For large data sets, this option is an efficient approach. To download the Data Import Wizard, visit [www.infoblox.com/import](https://www.infoblox.com/import).

In this example, when you create the corpxyz.com forward-mapping zone, you import zone data for the existing corpxyz.com zone from the legacy server at 10.1.5.3. When you create the 1.1.1.0/24 reverse-mapping zone, you also import the reverse-mapping zone records from the legacy server. After the appliance has both the forward- and reverse-mapping zone data, it converts the A and PTR records to Infoblox host records.

Creating a Name Server Group

1. Open an Internet browser window, enter `https://10.1.5.2`, and then log in to Grid Manager using the username `admin` and password `SnD34n534`.
2. From the **Data Management** tab, select the **DNS** tab -> **Name Server Groups** tab, and then click the Add icon -> **Name Server Group**.
3. In the **Name Server Group** wizard, complete the following:
   - **Name:** Enter `corpxyz` as the group name.
   - **Name Servers:** Click the Add icon -> **Primary**. In the **Add Primary** section, Grid Manager displays the host name of the independent appliance. Click Add. Grid Manager adds the independent system as the primary server.
   - **Stealth:** Clear this check box.
   - **Address:** Enter `2.2.2.2`.
   - **Comment:** Enter `corpxyz.com`.
4. Save the configuration and click **Restart** if it appears at the top of the screen.

Creating a Forward-Mapping Zone

**Note:** To import zone data, you must first create a zone and save it.

1. To create an authoritative zone, from the **Data Management** tab, select the **DNS** tab -> **Zones** tab, and then click the Add icon -> **Authoritative Zone**.
2. In the **Add Authoritative Zone** wizard, select **Add an authoritative forward-mapping zone**.
3. Click **Next** and complete the following:
   - **Name:** Enter `corpxyz.com`.
   - **Comment:** Enter **DNS zone**.
4. Click **Next** to assign a name server group to the zone.
5. Click the **Zones** tab, select the corpxyz.com check box, and then click the Edit icon.
6. In the **Authoritative Zone** editor, select the **Name Servers** tab, and then complete the following:
   - **Use this name server group:** Select this, and then select `corpxyz` from the drop-down list.
7. Save the configuration and click **Restart** if it appears at the top of the screen.

Importing Zone Data

1. To import zone data to the corpxyz.com zone that you created earlier, click the **Zones** tab, select the corpxyz.com check box, and then click **Import Zone** from the Toolbar.
2. In the **Import Zone** editor, complete the following:
• **Address**: Enter the IP address **10.1.5.3** of the DNS server from which you want to import zone data.

• **Create Hosts and Bulk Hosts during import**: Select this option to allow the appliance to merge imported records into hosts and bulk hosts. If you do not select this option, then resource records are imported one-to-one with each DNS record from the imported zone producing a corresponding DNS record on the NIOS appliance.

  • **Create PTR records for Hosts if necessary**: Select this to create host records from the imported address records, even if the corresponding PTR records or the authoritative reverse zones that would contain them, do not exist. If you do not select this option, then host records will be created for imported address records only if a corresponding PTR record exists.

  • **Create PTR records for Bulk Hosts if necessary**: Select this to create bulk host records from the imported address records, even if the corresponding PTR records or the authoritative reverse zones that would contain them, do not exist. If you do not select this option, then bulk host records will be created for the imported address records only if the corresponding PTR records exist.

3. Click **Import**.

4. After successfully importing the zone data, click corpxyz.com in the **Zones** tab. You can see all the imported forward-mapping zone data in the **Records** panel. Because you have not yet imported the reverse-mapping zone data, most of the records appear as A records.

5. To import the reverse-mapping zone data, from the **Zones** tab, click the **Add icon** -> **Authoritative Zone**.

6. In the **Add Authoritative Zone wizard**, select **Add an authoritative IPv4 reverse-mapping zone**.

7. Click **Next** and complete the following:

  • **IPv4 Network**: Enter **1.1.1.0**.
  • **Netmask**: Select **24** from the drop-down list.
  • **Comment**: Enter **Reverse-mapping zone**.

8. Click **Save & Close**.

9. To assign a name server group to the reverse-mapping zone, click the **Zones** tab, select the **1.1.1.in-addr.arpa** check box, and then click the **Edit icon**.

10. In the **Authoritative Zone editor**, select the **Name Servers** tab, and then complete the following:

    • **Use this name server group**: Select this, and then select corpxyz from the drop-down list.

11. Click **Save & Close**.

12. To import reverse-mapping zone data, click the **Zones** tab, select the corpxyz.com check box, and then click **Import Zone** from the **Toolbar**.

13. In the **Import Zone editor**, complete the following:

    • **Address**: Enter the IP address **10.1.5.3** of the DNS server from which you want to import zone data.

14. Click **Import**.

15. After successfully importing the zone data, click **1.1.1.in-addr.arpa** in the **Zones** tab. You can see all the imported reverse-mapping zone data in the **Records** panel.

16. Click corpxyz.com in the Forward Mapping Zones list. Because you have now imported both the forward- and reverse-mapping zone data, most of the records appear as host records.

17. Finally, you must remove the ns1 host record for the legacy server (value **1.1.1.3**). To remove it, select the ns1 check box (the host record for **1.1.1.3**), and then click the **Delete icon**.

### Designating the New Primary on the Secondary Name Server (at the ISP Site)

In this example, the external secondary name server is maintained by an ISP, so you must contact your ISP administrator to change the IP address of the primary (or **master**) name server. (If you have administrative access to the secondary name server, you can make this change yourself.) Because a firewall performing NAT exists between the secondary and primary name servers, specify the NAT address **1.1.1.2** for the primary name server instead of **10.1.5.2**.

#### Secondary BIND Server

1. Open the named.conf file using a text editor and set ns1 (with NAT address **1.1.1.2**) as the primary (or **master**) from which ns2 receives zone transfers in the named.conf file for the corpxyz.com zone:

   ```
   zone "corpxyz.com" in {
     type slave;
     masters {1.1.1.2};
     notify yes;
     file "/var/named/db.corpxyz.com";
   };
   ```

2. After editing the named.conf file, restart DNS service for the change to take effect.

#### Secondary Windows 2000/2003 Server

1. Click **Start** -> **All Programs** -> **Administrative Tools** -> **DNS**.
2. Click + (for ns2) -> + (for Forward Lookup Zones) -> corpxyz.com.
3. Right-click corpxyz.com, and then select **Properties** -> **General**.
4. On the **General page** in the corpxyz.com **Properties** dialog box, enter the following:

   • **Zone file name**: corpxyz.com.dns
1. **IP address**: Enter 1.1.1.2, and then click Add.

2. In the IP Address field, select 1.1.1.3 (the NAT IP address of the legacy DNS server), and then click Remove.

5. To save the configuration and close the `corpxyz.com Properties` dialog box, click OK.

---

### Configuring NAT and Policies on the Firewall

Change the NAT and policy settings on the firewall to allow bidirectional DNS traffic to and from `ns1.corpxyz.com` and NTP traffic from `ns1.corpxyz.com` to the NTP server at 10.120.3.10.

For example, enter the following commands on a Juniper firewall running ScreenOS 4.x or later:

```bash
set address dmz ns1 10.1.5.2/32
set address untrust ntp_server 10.120.3.10/32
set interface ethernet1 mip 1.1.1.2
host 10.1.5.2
set policy from dmz to untrust ns1 any dns permit
set policy from untrust to dmz any mip(1.1.1.2) dns permit
set policy from dmz to untrust ns1 ntp_server ntp permit
```

At this point, the new DNS server can take over DNS service from the legacy server. You can remove the legacy server and unset any firewall policies permitting traffic to and from 10.1.5.3.

### Deploying an Independent HA Pair

To deploy an independent HA pair, you cable the HA and LAN1, LAN1 (VLAN), or LAN2, LAN2 (VLAN) ports to the network and configure the IP settings for these ports and the VIP address within the same subnet. For more information about HA pairs, see *About HA Pairs*.

The default LAN1 or LAN2 settings are as follows:

- IP address: 192.168.1.2
- Netmask: 255.255.255.0

You can configure an HA pair using the Infoblox NIOS Startup Wizard. IPv4 and IPv6 network values are supported for the NIOS Startup Wizard and for HA Pair configuration. The NIOS appliance MGMT port also can be configured to support an IPv6 address.

- **Requirements**: HTTPS connections from your management system to the Ethernet ports on the two appliances.
- **Advantage**: The startup wizard provides step-by-step guidance for configuring the network settings of the VIP address and HA and LAN1 or LAN2 (VLAN) ports on both nodes, for setting the host name, admin password, and system clock, and—if using NTP (Network Time Protocol)—for enabling the HA pair as an NTP client.

### Using the Infoblox NIOS Startup Wizard to Configure an HA Pair

When you first make an HTTPS connection to the NIOS appliance, the Infoblox NIOS Startup Wizard guides you through various deployment options, basic network settings, and opportunities for changing the password of the superuser `admin` and for setting the system clock.

#### Configuring the Connecting Switch

To ensure that VRRP (Virtual Router Redundancy Protocol) works properly, configure the following settings at the port level for all the connecting switch ports (HA, LAN1, LAN1 (VLAN), LAN2, and LAN2 (VLAN)):

- **Spanning Tree Protocol**: Disable. For vendor specific information, search for "HA" in the Infoblox Knowledge Base system at [https://support.infoblox.com](https://support.infoblox.com).
- **Trunking**: Disable
- **EtherChannel**: Disable
- **IGMP Snooping**: Disable
- **Port Channeling**: Disable
- **Speed and Duplex settings**: Match these settings on both the Infoblox appliance and switch
- **Disable other dynamic and proprietary protocols that might interrupt the forwarding of packets**

**Note**: By default, a NIOS appliance automatically negotiates the optimal connection speed and transmission type (full or half duplex) on the physical links between its LAN1, HA, and MGMT ports and the Ethernet ports on the connecting switch. If the two appliances fail to autonegotiate the optimal settings, see *Modifying Ethernet Port Settings* for steps you can take to resolve the problem.

### Putting Both Nodes on the Network

1. Use one of the methods described in *Deploying a Single Independent Appliance* to configure the network settings of the LAN1 port of each node so that they are on the same subnet and you can reach them across the network.

2. Cable the LAN1 port and the HA port on each node to the network switch.

   **Note**: The Ethernet ports on the TE-810, TE-820, TE-1410, TE-1420, TE-2210, TE-2220, and IB-4010 appliances are autosensing, so you can use either a straight-through or cross-over Ethernet cable for these connections.

3. Cable your management system to the network switch.
Configuring Node 1

1. Open an Internet browser window and enter https://<the IP address of the appliance> to make an HTTPS connection to the first node. For information about supported browsers, see Supported Browsers.

2. Enter the default username and password (admin and infoblox) on the Grid Manager login page, and then click Login or press Enter. For information, see Logging in to the GUI.

3. Read the Infoblox End-User License Agreement, and then click I Accept to proceed. Grid Manager may take a few seconds to load your user profile.

4. In the first screen of the Grid Setup wizard, select Configure a Grid Master and click Next.

5. Specify the following:
   - **Grid Name**: Type the name of the Grid. The default name is Infoblox.
   - **Shared Secret**: Enter the shared secret that both nodes use to authenticate each other when establishing a VPN tunnel for ensuing bioboxSYNC traffic. The default shared secret is test.
   - **Confirm Shared Secret**: Enter the shared secret again.
   - **Host Name**: Enter a valid domain name for the node.
   - **Type of Network Connectivity**: Select the type of network connectivity from the drop-down list:
     - **IPv4 and IPv6**: Select this to configure a dual mode HA pair.
     - **IPv4**: Select this to configure an IPv4 HA pair.
     - **IPv6**: Select this to configure an IPv6 HA pair.
   - **Select Yes in the Is the Grid Master an HA pair field for the first appliance of the HA pair.
   - **Send HA and Grid Communication over**: Select either IPv4 or IPv6. This field is displayed only when you configure a dual mode (IPv4 and IPv6) HA pair.

6. Click Next and complete the following to set properties for the first node:
   - **Virtual Router ID**: Enter the VRID (virtual router ID). This must be a unique VRID number—from 1 to 255—for this subnet.
   - **Ports and Addresses**: This table lists the network interfaces depending on the type of network connectivity. For IPv4 HA pair, specify the network information for VIP (IPv4), Node1 HA (IPv4), Node2 HA (IPv4), Node1 LAN1 (IPv4), and Node2 LAN1 (IPv4) interfaces. For IPv6 HA pair, specify the network information for VIP (IPv6), Node1 LAN1 (IPv6), and Node2 LAN1 (IPv6) interfaces.
     - For a dual mode HA pair, if you select IPv4 in the Send HA and Grid Communication over field in step 2 of the NIOS Startup wizard, specify the network information for the following interfaces: VIP (IPv4), Node1 HA (IPv4), Node1 LAN1 (IPv4), Node2 HA (IPv4), Node2 LAN1 (IPv4), VIP (IPv6), Node1 LAN1 (IPv6), and Node2 LAN1 (IPv6) ports. If you select IPv6 in the Send HA and Grid Communication over field in step 2 of the NIOS Startup wizard, specify the network information for the following interfaces: VIP (IPv4), Node1 LAN1 (IPv4), Node2 LAN1 (IPv4), VIP (IPv6), Node1 LAN1 (IPv6), and Node2 LAN1 (IPv6).

   Click the empty fields and complete the following information:
   - **Interface**: Displays the name of the interface. You cannot modify this.
   - **Address**: Type the IPv4 or IPv6 address depending on the type of interface.
   - **Subnet Mask (IPv4) or Prefix Length (IPv6)**: Specify an appropriate subnet mask for IPv4 address or prefix length for IPv6 address. The prefix length ranges from 2 to 127.
   - **Gateway**: Type the IPv4 or IPv6 address of the default gateway depending on the type of interface. For IPv6 interface, you can also type Automatic to enable the appliance to acquire the IPv6 address of the default gateway and the link MTU from router advertisements.
   - **Port Settings**: Select the port settings from the drop-down list. The list contains all settings supported by the hardware model. The default is Automatic. The appliance automatically detects the port settings.

7. Click Next and complete the following to set admin password:
   - **Yes**: To change the default password.
   - **No**: To keep the default password.
     - If you select Yes, complete the following:
     - **Password**: Enter a password for the superuser admin account. The password cannot contain spaces and it must be at least four characters long. The password is case-sensitive.
   - **Retype Password**: Enter the same password.

8. Click Next and complete the following to configure time settings:
   - **Time Zone**: Select the applicable time zone from the drop-down list. The default is (UTC) Coordinated Universal Time.
   - **Would you like to enable NTP?**: Select Yes to synchronize the time with external NTP servers. Click the Add icon. Grid Manager adds a row to the NTP Server table. Click the row and enter either the IPv4 or IPv6 address or the resolvable host name of an NTP server. You can view a list of public NTP servers at ntp.isc.org.
   - **Select No to specify a date and time.**
     - **Date**: Enter the data in YYYY-MM-DD format. You can also click the calendar icon to select a date from the calendar widget.
     - **Time**: Enter the time in HH:MM:SS AM/PM format. You can also click the clock icon to select a time from the drop-down list.

9. Click Next to view the summary of the configuration. Review the information and verify that it is correct. You can change the information you entered by clicking Previous to go back to a previous step.

10. Click Finish.
Configuring Node 2

1. Open an Internet browser window and enter `https://<the IP address of the appliance>` to make an HTTPS connection to the second node. For information about supported browsers, see Supported Browsers.

Several certificate warnings may appear during the login process because the preloaded certificate is self-signed and has the hostname `www.infoblox.com`, which may not match the destination IP address you entered in step 1. To stop the warning messages from occurring each time you log in to Grid Manager, you can generate a new self-signed certificate or import a third-party certificate with a common name that matches the FQDN (fully qualified domain name) of the appliance. For information, see Creating a Login Banner.

2. Enter the default username and password (admin and infoblox) on the Grid Manager login screen, and then click Login or press Enter. For information, see Logging in to the GUI.

3. Read the Infoblox End-User License Agreement, and then click I Accept to proceed. Grid Manager may take a few seconds to load your user profile.

4. In the first screen of the NIOS Setup Wizard, complete the following:
   - **Type of Network Connectivity**: Select the type of network connectivity from the drop-down list:
     - IPv4 and IPv6: Select this to configure a dual mode HA pair.
     - IPv4: Select this to configure an IPv4 HA pair.
     - IPv6: Select this to configure an IPv6 HA pair.
   - **Select Configuring an HA pair** to configure an independent HA pair and click **No** to configure the first node of an HA pair.

5. Click Next and complete the following to configure network settings:
   - **HA Virtual IP address**: Enter the VIP (virtual IP) address and its netmask.
   - **HA Pair Name**: Enter a name for the HA pair. The default name is Infoblox. Ensure that you use the same name as the first node.
   - **Shared Secret**: Enter a text string that both nodes use as a shared secret to authenticate each other when establishing a VPN tunnel. The default shared secret is test. This must be the same shared secret that you entered on the first appliance.
   - **Show Password**: Click this to display the shared secret. Clear it to conceal the shared secret.

6. Click Next, and then complete the following to set properties for the second appliance:
   - **IP Address**: Enter the IPv4 or IPv6 address of the appliance.
   - **Subnet Mask**: Enter the subnet mask of the appliance.
   - **Prefix Length**: Enter the prefix length if you have entered the IPv6 address in the **IP Address** field. The prefix length ranges from 2 to 127.
   - **Gateway**: Enter the IP address of the gateway of the subnet of the interface.

7. Click Next to view the summary of the configuration. Review the information and verify that it is correct. You can change the information you entered by clicking Previous to go back to a previous step.

8. Click Finish.

The setup of the HA pair is complete. When you next make an HTTPS connection to the HA pair, use the VIP address. The communication protocol for all the services in a dual mode (IPv4 and IPv6) HA appliance is the same protocol as the one used for VRRP advertisements. For example, if you select IPv4 in the Send HA and Grid Communication Over field on the first screen of the NIOS Setup wizard, then IPv4 is set as the communication protocol for all the services. However, you can override the communication protocol for all the services in a dual mode HA pair. For information, see Changing the Communication Protocol for a Dual Mode Independent Appliance.

**Configuration Example: Configuring an HA Pair for Internal DNS and DHCP Services**

In this example, you set up an HA pair of NIOS appliances to provide internal DNS and DHCP services. The HA pair answers internal queries for all hosts in its domain (corpxyz.com). It forwards internal queries for external sites to ns1.corpxyz.com at 10.1.5.2 and ns2.corpxyz.com at 2.2.2.2. It also uses DHCP to provide dynamic and fixed addresses. You can deploy the HA appliance in IPv4, IPv6 or dual mode (IPv4 and IPv6), but the configuration example uses IPv4 addresses.

The HA pair consists of two appliances (nodes). The IP addresses of the VIP (virtual IP) address of the HA pair and the HA and LAN1 ports on each node, are as follows:

<table>
<thead>
<tr>
<th>HA Pair IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP 10.1.4.10 (the address that the active node of the HA pair uses)</td>
</tr>
<tr>
<td>Node 1</td>
</tr>
<tr>
<td>LAN1 10.1.4.6</td>
</tr>
<tr>
<td>HA 10.1.4.7</td>
</tr>
</tbody>
</table>

The virtual router ID number for the HA pair is 150. The ID number must be unique for this network segment. When you create the corpxyz.com zone on the HA pair, you import DNS data from the legacy server at 10.1.4.11.

*Figure 6.6 Example 2 Network Diagram*
An HA pair of NIOS appliances provides internal DNS services. It answers internal queries for all hosts in its domain. It forwards internal queries for external sites to ns1 and ns2. It also serves DHCP, providing both dynamic and fixed addresses. For information on configuring the NIOS appliance as a primary DNS server, see Configuration Example: Deploying a NIOS Appliance as a Primary DNS Server.

Cabling Appliances to the Network and Turning On Power
Connect Ethernet cables from the LAN1 and HA ports on both NIOS appliances to a switch in the server network and turn on the power for both appliances. For information about installing and cabling the appliance, refer to the user guide or installation guide that ships with the product.

Specifying Initial Network Settings
Before you can configure the appliances through Grid Manager, you must be able to make a network connection to them. The default network settings of the LAN1 port are 192.168.1.2/24 with a gateway at 192.168.1.1 (the HA and MGMT ports do not have default network settings). To change these settings, you can use the LCD or make a console connection to each appliance.

Node 1
Using the LCD or console port on one of the appliances, enter the following information:

- IP Address: 10.1.4.6 (for the LAN1 port)
- Netmask: 255.255.255.0
- Gateway: 10.1.4.1

Node 2
Using the LCD or console port on the other appliance, enter the following information:
• IP Address: 10.1.4.8 (for the LAN1 port)
• Netmask: 255.255.255.0
• Gateway: 10.1.4.1

After you confirm your network settings, the Infoblox GUI application automatically restarts.

Specifying Appliance Settings

When you make the initial HTTPS connection to a NIOS appliance, the Infoblox NIOS Startup Wizard guides you through the basic deployment of the appliance on your network. To set up an HA pair, you must connect to and configure each appliance individually.

Node 1

1. Open an Internet browser window and enter https://10.1.4.6.
2. Accept the certificate when prompted. Several certificate warnings may appear during the login process. This is normal because the preloaded certificate is self-signed and has the hostname www.infoblox.com, which does not match the destination IP address you entered in step 1. To stop the warning messages from occurring each time you log in to Grid Manager, you can generate a new self-signed certificate or import a third-party certificate with a common name that matches the FQDN (fully-qualified domain name) of the appliance. This is a very simple process. For information about certificates, see Creating a Login Banner.
3. Enter the default username and password (admin and infoblox) on the Grid Manager login page, and then click Login or press Enter. For information, see Logging in to the GUI.
4. Read the Infoblox End-User License Agreement, and then click I Accept to proceed. Grid Manager may take a few seconds to load your user profile.
5. In the first screen of the NIOS Setup wizard, complete the following:
   • Type of Network Connectivity: Select IPv4 as the communication protocol from the drop-down list.
   • Select Configuring an HA pair and click Yes to configure the first appliance.
   • Send HA and Grid Communication over: Select IPv4 from the drop-down list for VRRP advertisements.
6. In the NIOS Startup wizard, select Configuring an HA pair. Click Yes to configure the first appliance.
7. Click Next and complete the following to configure network settings:
   • Host Name: Enter ns3.corpxyz.com.
   • HA Pair Name: Use the default name Infoblox.
   • Shared Secret: Enter 37eeT1d.
8. Click Next and complete the following to set properties for the first node:
   • Virtual Router ID: Enter 150.
   • Required Ports and Addresses: In the table, click the empty fields and enter the following information for each corresponding interface in the table:
     • VIP (IPv4): 10.1.4.10
     • Node 1 HA (IPv4): 10.1.4.7
     • Node 2 HA (IPv4): 10.1.4.9
     • Node 1 LAN1 (IPv4): 10.1.4.6
     • Node 2 LAN1 (IPv4): 10.1.4.8
     • Subnet Mask: 255.255.255.0
     • Gateway: 10.1.4.1

   Note: Some fields are prepopulated by Grid Manager based on the existing configuration of the appliance. All fields are required.
9. Click Next and complete the following to set admin password:
   • Would you like to set admin password?: Click No.
10. Click Next and complete the following to configure time settings:
   • Time Zone: Select UMT – 8:00 Pacific Time (US and Canada), Tijuana from the drop-down list.
   • Would you like to enable NTP?: Select Yes to synchronize the time with external NTP servers, and then click the Add icon.
      Grid Manager adds a row to the NTP Server table. Click the row and enter 10.120.3.10 in the NTP Server field.
11. Click Next to view the summary of the configuration. Review the information and verify that it is correct. You can change the information you entered by clicking Previous to go back to a previous step.
12. Click Finish.

Node 2

1. From the System tab, select the System Manager tab, and then click System Properties -> Setup Wizard from the Toolbar.
2. In the first screen of the NIOS Setup wizard, complete the following:
   • Type of Network Connectivity: Select IPv4 as the communication protocol from the drop-down list.
   • Select Configuring an HA pair and click Yes for configuring node 2 of the HA pair.
3. In the NIOS Startup wizard, select Configuring an HA pair to configure an independent HA pair. Click No for configuring node 2 of the HA pair.
4. Click Next, and then complete the following to configure network settings:
   • HA Virtual IP address: Enter 10.1.4.10.
   • HA Pair Name: Use the default name Infoblox.
4. Click **Next**, and then complete the following to set properties for the second appliance:
   - **IP Address**: Enter **10.1.4.8**.
   - **Subnet Mask**: Enter **255.255.255.0**.
   - **Gateway**: Enter **10.1.4.1**.
5. Click **Next** to view the summary of the configuration. Review the information and verify that it is correct. You can change the information you entered by clicking **Previous** to go back to a previous step.
6. Click **Finish**.

The setup of the HA pair is complete. From now on, when you make an HTTPS connection to the HA pair, use the VIP address 10.1.4.10.

### Enabling Zone Transfers

To allow the NIOS appliance to import zone data from the legacy server at 10.1.4.11, you must configure the legacy server to allow zone transfers to the appliance at 10.1.4.10.

#### Legacy BIND Server

1. Open the named.conf file using a text editor and change the allow-transfer statement to allow zone transfers to the appliance at 10.1.4.10. For a sample of the required changes to the named.conf file, see Legacy BIND Server.
2. After editing the named.conf file, restart DNS service for the change to take effect.

#### Legacy Windows 2000/2003 Server

Navigate to the **corpxyz.com Properties** dialog box, and add 10.1.4.10 to the list of IP addresses to which you want to allow zone transfers. For more detailed navigation and configuration instructions, see Legacy Windows 2000/2003 Server.

### Importing Zone Data

You can import zone data from a legacy server to an independent HA pair, as described in Importing Zone Data on an Independent Appliance. Use the following information:

- Forward-mapping zone: **corpxyz.com**
- Import zone from: **10.1.4.11**
- Reverse-mapping zone: **1.1.1.0**

### Defining Networks, Reverse-Mapping Zones, DHCP Ranges, and Infoblox Hosts

In this task, you enter data manually. For large data sets, you have the option of using the Data Import Wizard for loading DNS and DHCP configurations and data to make the process more efficient. To download the Data Import Wizard, visit www.infoblox.com/import/.

### Networks

You can create all the subnetworks individually (which in this example are 10.1.1.0/24, 10.1.2.0/24, 10.1.4.0/24, and 10.1.5.0/24), or you can create a parent network (10.1.0.0/16) that encompasses all the subnetworks and then use the Infoblox split network feature to create the individual subnetworks automatically. The split network feature accomplishes this by using the IP addresses that exist in the forward-mapping zones to determine which subnets it needs to create. This example uses the split network feature. For information about creating networks, see Configuring IPv4 Networks.

1. From the **Data Management** tab, select the **IPAM** tab, and then click **Add -> Add IPv4 Network** from the Toolbar.
2. In the **Add Network** wizard, complete the following:
   - **Address**: **10.1.0.0**
   - **Netmask**: Use the netmask slider to select the /16 (255.255.0.0) netmask.
3. Click **Next** to select a server. Click the **Add** icon. Grid Manager displays ns3.corpxyz.com in the table.
4. Click **Save & Close**.
5. In the **IPAM** tab, select the 10.1.0.0/16 check box, and then select **Split** from the Toolbar.
6. In the **Split Network** dialog box, complete the following:
   - **Subnetworks**: Move the slider to 24.
   - **Immediately Add**: Select **Only networks with ranges and fixed addresses**.
   - **Automatically create reverse-mapping zones**: Select this check box.
7. Click **OK**.

The appliance creates the following 24-bit subnets for the imported Infoblox hosts:
8. From the IPAM tab, click the 10.1.1.0/24 check box, and then click the Edit icon.
9. In the DHCP Network editor, enter information in the following tabs:

**General**
- **Comment:** MGT

**Server Assignment**
- Add `ns3.corpxyz.com` as a server.

10. Click Save & Close.

11. To modify the other networks, repeat steps #8 – 10 for each network and use the following information:

**10.1.2.0/24 Network:**
- **Comment:** Dev
- **Server Assignment:** `ns3.corpxyz.com`

**10.1.4.0/24 Network:**
- **Comment:** Server
- **Server Assignment:** `ns3.corpxyz.com`

**10.1.5.0/24 Network:**
- **Comment:** DMZ
- **Server Assignment:** `ns3.corpxyz.com`

### DHCP Ranges

1. From the Data Management tab, select the DHCP tab -> Networks tab -> 10.1.1.0/24, and then click Add -> DHCP Range from the Toolbar.
2. In the Add Range wizard, complete the following:
   - **Start:** 10.1.1.10
   - **End:** 10.1.1.50
3. Click Next, and then select Server. Grid Manager displays `ns3.corpxyz.com` as the assigned member.
4. Click Save & Close.
5. In the Networks tab, click 10.1.2.0/24, and then click Add -> DHCP Range from the Toolbar.
6. In the Add Range wizard, complete the following:
   - **Start:** 10.1.2.10
   - **End:** 10.1.2.50
7. Click Next, and then select Server. Grid Manager displays `ns3.corpxyz.com` as the assigned member.
8. Click Save & Close.

### Infoblox Hosts

Defining both a MAC and IP address for an Infoblox host definition creates a DHCP host entry—like a fixed address—that you can manage through the host object. To add a MAC address to each host record that the appliance created when you imported forward- and reverse-mapping zone records:

1. From the Data Management tab, select the IPAM tab -> 10.1.1.0/24 -> 10.1.1.2.
2. In the Related Objects tab, select the check box of the host record, and then click the Edit icon.
3. In the Host Record editor, click the MAC Address field, and then enter the following:
   - **MAC Address:** 00:00:00:aa:aa:aa
4. Click Save & Close.
5. Follow steps 1 – 4 to modify hosts with the following information:

**printer2**
- **IP Address:** 10.1.2.2
- **MAC Address:** 00:00:00:bb:bb:bb

**storage1**
- **IP Address:** 10.1.4.2
- **MAC Address:** 00:00:00:dd:dd:dd

**storage2**
Defining Multiple Forwarders

Because ns3.corpxyz.com is an internal DNS server, you configure it to forward DNS queries for external DNS name resolution to the primary and secondary DNS servers—ns1.corpxyz.com at 10.1.5.2 and ns2.corpxyz.com at 2.2.2.2.

1. From the Data Management tab, select the DNS tab, and then select System DNS Properties from the Toolbar.
2. In the System DNS Properties editor, click the Add icon in the Forwarders tab. Grid Manager adds a row to the table. Complete the following:
   - Address: Type 2.2.2.2. Click Add again to add another forwarder.
   - Address: Type 10.1.5.2.
3. Save the configuration and click Restart if it appears at the top of the screen.

Each of the forwarders is assigned a random response time. The appliance sends the initial outbound query to the forwarder that has the lowest response time. If the first forwarder does not reply, the appliance tries the one with the next lowest random response time. The appliance adjusts and keeps track of the response times of the forwarders, and uses the quicker one for future queries. If the quicker forwarder does not respond, the appliance then uses another one.

Enabling Recursion on External DNS Servers

Because the HA pair forwards outbound queries to the two external DNS servers ns1.corpxyz.com (10.1.5.2) and ns2.corpxyz.com (2.2.2.2) for resolution, you must enable recursion on those servers. When a DNS server employs recursion, it queries other DNS servers for a domain name until it either receives the requested data or an error that the requested data cannot be found. It then reports the result back to the server that queried—in this case, the internal DNS server ns3.corpxyz.com (10.1.4.10), which in turn reports back to the DNS client.

Infoblox Server in the DMZ Network (ns1.corpxyz.com, 10.1.5.2)

1. From the Data Management tab, select the DNS tab, and then click System DNS Properties from the Toolbar.
2. In the System DNS Properties editor, select the Allow Recursion check box from the Queries tab, and then click the Add icon -> IPv4 Address. Grid Manager adds a row to the Allow recursive queries from table. Complete the following:
   - Permission: Select Allow from the drop-down list.
   - Name: Enter 10.1.1.52.
3. Save the configuration and click Restart if it appears at the top of the screen.

BIND Server at ISP Site (ns2.corpxyz.com, 2.2.2.2)

1. Open the named.conf file using a text editor and change the recursion and allow-recursion statements to allow recursive queries from 1.1.1.8 (the NAT address of ns3).

```plaintext
options {
    zone-statistics yes;
}
```
directory "/var/named/named_conf"; version"";
recursion yes;
listen-on { 127.0.0.1; 2.2.2.2; };
...
allow-recursion {1.1.1.8};
transfer-format many-answers;
};

2. After editing the named.conf file, restart DNS service for the change to take effect.

Windows 2000/2003 Server at ISP Site (ns2.corpxyz.com, 2.2.2.2)

1. Click Start -> All Programs -> Administrative Tools -> DNS.
2. Right-click ns3, and then select Properties -> Advanced.
3. On the Advanced page in the ns3 Properties dialog box, clear the Disable recursion check box.
4. To save the configuration change and close the ns3 Properties dialog box, click OK.

Modifying the Firewall and Router Configurations

Configure the firewall and router in your internal network to allow the following DHCP, DNS, and NTP traffic:

- To allow messages to pass from the DHCP clients in the DMZ—the web, mail, and FTP servers—to ns3 in the Server network, configure policies and DHCP relay agent settings on the firewall.
- To forward DHCP messages from DHCP clients in the MGT and Dev networks to ns3 in the Server network, configure relay agent settings on the router.
- To translate the private IP address of ns3 (10.1.4.10) to the public IP address (1.1.1.8) when forwarding DNS queries from ns3 to ns2, set a MIP (mapped IP) address on the firewall.
- To allow DNS queries from ns3 to ns1 and ns2 and NTP traffic from ns3 to the NTP server, configure firewall policies.

Firewall

For example, enter the following commands on a Juniper firewall running ScreenOS 4.x or later:

**DHCP Relay Configuration**

```
set address trust ns3 10.1.4.10/32
set interface ethernet2 dhcp relay server-name 10.1.4.10
set policy from dmz to trust ns1 ns3 DHCP-Relay permit
```

**DNS Forwarding**

```
set interface ethernet1 mip 1.1.1.8 host 10.1.4.10
set policy from trust to untrust ns3 ns2 dns permit
set policy from trust to dmz ns3 ns1 dns permit
```

**NTP**

```
set policy from dmz to untrust ns1 ntp_server ntp permit
```

Router

For example, enter the following commands on a Cisco router running IOS for release 12.x or later:

**DHCP Relay Configuration**

```
interface ethernet1
   ip helper-address 10.1.4.10 interface ethernet2
ip helper-address 10.1.4.10
```

Enabling DHCP and Switching Service to the NIOS Appliance

With the Infoblox in place and the firewall and router configured for relaying DHCP messages, you can switch DHCP service from the legacy DHCP server at 10.1.4.11 to the HA pair at 10.1.4.10 (VIP address).

**Tip:** To minimize the chance of duplicate IP address assignments during the transition from the legacy DHCP server to the appliance, shorten all
lease times to a one-hour length in advance of the DHCP server switch. Then, when you take the legacy DHCP server offline, the DHCP clients quickly move to the new server when their lease renewal efforts fail and they broadcast DHCPDISCOVER messages. To determine how far in advance you need to shorten the lease length, find the longest lease time (for example, it might be two days). Then change the lease length to one hour at a slightly greater interval of time before you plan to switch DNS service to the appliance (for example, three days before the switch over). By changing the lease length this far in advance, you can be sure that all DHCP leases will be one-hour leases at the time of the switch-over. If the longest lease length is longer—such as five days—and you want to avoid the increased amount of traffic caused by more frequent lease renewals over a six-day period, you can also employ a stepped approach: Six days before the switch-over, change the lease lengths to one-day leases. Then two days before the switch-over, change them to one-hour leases.

1. Open an Internet browser window, enter https://10.1.4.10, and then log in to the appliance using the username admin and password SnD34n534.
2. From the Data Management tab, select the DHCP tab, and then click Start from the Toolbar.
3. In the Start Member DHCP Service dialog box, click Yes. The HA pair is ready to provide DHCP service to the network.
4. Take the legacy DHCP server at 10.1.4.11 offline.
   When the DHCP clients are unable to renew their leases from the legacy DHCP server, they broadcast DHCPDISCOVER messages to which the new DHCP server responds.

Managing and Monitoring

Infoblox provides tools for managing IP address usage and several types of logs to view events of interest and DHCP and DNS data. After configuring the appliance, you can use the following resources to manage and monitor IP address usage, DNS and DHCP data, and administrator and appliance activity.

IPAM (IP Address Management)

IPAM offers the following services:

- Simple IP address modification – Within a single IP address-centric data set, you can modify the Infoblox host, DHCP, and DNS settings associated with that IP address.
- Address type conversion — Through IPAM functionality, you can make the following conversions:
  - Currently active dynamic addresses to fixed addresses, reserved addresses, or Infoblox hosts.
  - Fixed addresses to reservations or hosts.
  - Reservations to hosts.
- Device classification — You can make detailed descriptions of appliances in DHCP ranges and appliances defined as Infoblox hosts and as fixed addresses.
- Three distinct views of IP address usage – To monitor the usage of IP addresses on your network, you can see the following different views:
  - High-level overall network view: From the Data Management tab, select the IPAM tab -> member. You can view the network usage in the Net Map or List view. You can also drill down to specific IP address to get detailed information.
  - DHCP lease history records: From the Data Management tab, select the DHCP tab -> Leases tab -> Lease History.

Logs

The following are some useful information:

- Logs, as described in Monitoring the Appliance.
  - Audit Log – Contains administrator-initiated events.
  - System Log – Contains events related to hardware and software operations.
- DNS statistics, as described in Configuring DNS Services.
  - DNS Configuration – Contains DNS server settings for the Infoblox DNS server.
  - Zone Statistics – Contains the results of all DNS queries per zone.
- DHCP information, as described in Configuring DHCP Properties.
  - DHCP Configuration – Contains DHCP server settings and network, DHCP range, and host settings for the Infoblox DHCP server.
  - DHCP Leases – Contains a real-time record of DHCP leases.
  - DHCP Lease History – Contains an historical record of DHCP leases.
  - DHCP Statistics – Contains the number of currently assigned static and dynamic addresses, and the high and low watermarks per network.
  - Network Statistics – Contains the number of static hosts, dynamic hosts, and available hosts per network.

Verifying the Deployment

After you deploy a single independent appliance or HA pair, you can make an HTTPS connection to it, log in, and check its status.

Single Independent Appliance

From the Dashboard, check the appliance status in the System Status widget. For information, see Member Status (System Status).
• If the Status icon is green, the appliance has a network connection and is operating properly.
• If the Status icon is red, there is a problem. To determine what it is, look at the system log file for this appliance by selecting the **Administration** tab -> **Logs** tab -> **Syslog**.

**Independent HA Pair**

1. Make an HTTPS connection to the VIP address of the HA pair, log in, and check the status of both nodes.
2. From the Dashboard, check the appliance status in the **SystemStatus** widget. For information, see **MemberStatus (System Status)**.

   • If the Status icon is green, both nodes have connectivity with each other and are operating properly.
   • If the Status icon is yellow, the two nodes are in the process of forming an HA pair.
   • If the Status icon is red, the passive node is offline or there is a problem. To determine what it is, look at the system log file by selecting the **Administration** tab -> **Logs** tab -> **Syslog**. You can also gather information from the **System** tab -> **SystemManager** tab. For information, refer to the online Help.

**Infoblox Tools for Migrating Bulk Data**

Typically, the next step after cabling a single independent appliance to a network and configuring its network settings—or cabling two independent appliances to a network and configuring them as an HA pair—is to import data from legacy DNS, DHCP, and TFTP servers. Infoblox provides several tools to accomplish this:

- The CSV import feature allows you to import DNS, DHCP, and IPAM data through Grid Manager. You can add, overwrite, or merge data using this feature. The appliance updates the database based on import settings and the data you specify in the data files. From the **Data Management** tab of Grid Manager, you can access the **Import Manager** editor from which you start a data import. You can also export existing data to a CSV file. You can use this file to modify data, and then re-import the data into the database using the CSV import feature. For information, see **About CSV Import**.
- The Infoblox Data Import Wizard is a useful tool that simplifies the importation of DNS, DHCP and IPAM, and TFTP settings and data into a NIOS appliance. For large data sets, this option is an efficient approach. To download the Data Import Wizard, visit [www.infoblox.com/import](http://www.infoblox.com/import).
- For smaller DNS data sets, you can use the zone import feature, which allows you to import data on a per-zone basis (see **Importing Zones**).

**Chapter 7 Deploying Cloud Network Automation**

With valid licenses installed, you can configure Cloud Platform Appliances in your Grid to provide DNS and DHCP services for virtual machines and network devices deployed through a CMP (Cloud Management Platform). To deploy a Grid that contains cloud members, it is important to understand the required components, how to configure the members to enable Cloud Network Automation, and which cloud API objects are supported.

This chapter contains the following sections:

- **Introduction to Cloud Network Automation**
  - Licensing Requirements
  - Licensing Configurations
  - Administrative Permissions
  - Supported Cloud Platform Appliance Models
  - Setting Up Cloud Network Automation
- **About Cloud API Service**
  - Starting the Cloud API Service
  - Monitoring Cloud API Service
  - Cloud API Request Process
  - Supported Cloud API Objects
  - Proxying Cloud API Requests
- **About Authority Delegation**
  - Guidelines for Delegating Authority
  - Delegating Authority for Cloud Objects
- **Configuring Grid and Member Cloud API Properties**
- **Extensible Attributes for Cloud Objects**
- **Extensible Attributes for Tags in AWS and Azure**
- **Viewing Cloud Objects**
  - Viewing All Tenants
  - Viewing All Cloud Networks
  - Viewing All Cloud VMs
  - Viewing All Cloud Platform Members

**Introduction to Cloud Network Automation**

The Infoblox Cloud Network Automation solution automates IPAM (IP address management) for physical and virtual network devices on your CMP (whether it is private, public, or hybrid). Instead of manually provisioning IP addresses and DNS name spaces for network devices and interfaces, you can use Cloud Network Automation to leverage DNS and DHCP features of the Grid to manage your cloud networks. When your
Cloud Network Automation consists of a large number of servers and VMs (virtual machines) that have multiple associated network interfaces, manually provisioning and

dev-provisioning IP addresses and managing DNS and DHCP data can become error-prone. Utilizing Cloud Network Automation can minimize human errors by streamlining IPAM, improve visibility of your cloud networks, and maximize the flexibility and efficiency that virtualization offers in your cloud environment.

To maximize the capability of Cloud Network Automation, ensure that you understand the operations of Cloud Network Automation and how to deploy necessary components to suit your network topology and CMP. For detailed information about the Cloud Network Automation operations, see **Cloud Network Automation Operations**.

**Cloud Network Automation Operations**

Figure 7.1 shows the basic concept and operations of Cloud Network Automation, which includes two major components: the Grid Master that has a Cloud Network Automation license installed and one or more Cloud Platform Appliances that provide the ability to process API requests. Instead of sending all API requests to the Grid Master, you can send requests directly to the Cloud Platform Appliances. The Cloud Network Automation license installed on the Grid Master enables visibility and reporting on cloud tenants, VM IP addresses, and DNS record allocation. This license can be used in conjunction with Cloud Platform Appliances to provide local survivability and additional scalability of cloud API requests within individual data centers, or it can be used with an existing Grid Master servicing all cloud API requests.

A Cloud Platform Appliance is a Grid member designed and dedicated to accept and process WAPI (RESTful API) requests related to cloud objects, in addition to serving DNS and DHCP protocols. You can deploy multiple Cloud Platform Appliances within your Grid to scale the processing of API requests or to provide redundancy. Cloud Platform Appliances include built-in HTTPS proxy capability that redirects cloud API requests to the appropriate Cloud Platform Appliance or to the Grid Master for processing. In other words, cloud API requests can be sent to any of the Cloud Platform Appliances within the Grid and the call is either processed locally or transparently forwarded to the appliance that is authoritative for the object referenced in the cloud API request. For information about supported Cloud Platform Appliances and their specifications, see **Supported Cloud Platform Appliance Models**. Once you have installed the Cloud Platform license on the appliance, fixed address configuration takes effect immediately by default and no DHCP service restart is required on the Cloud Platform Appliance. For information about this feature, see **Configuring Fixed Addresses without Restarting DHCP Service**. You can also add and delete IPv4 and IPv6 fixed addresses, reservations, and host records within any delegated IP address ranges through Grid Manager (the Infoblox GUI), in addition to using cloud API calls. For more information, see **Managing IPv4 DHCP Data** and **Managing IPv6 DHCP Data**.

On the CMP, you can either deploy a cloud adapter and use it as the cloud API client for sending cloud API requests to the Cloud Platform Appliances, or you can customize your CMP to make cloud API requests directly to Cloud Platform Appliances or to the Grid Master. The cloud adapter can be configured to send API requests always to a single Cloud Platform Appliance or to different Cloud Platform Appliances to handle situations where the primary Cloud Platform Appliance may not be available or to distribute API load among multiple Cloud Platform Appliances.

Infoblox Cloud Network Automation supports the following cloud adapters: Infoblox IPAM Plug-In for VMware, OpenStack Adapter, and AWS (Amazon Web Services) API Proxy. For information about the IPAM Plug-In for VMware and OpenStack Adapter, refer to their respective Quick Start Guides. For information about the AWS API Proxy and how to set up AWS configurations, refer to the InfobloxInstallationGuidesNIOStoAWS.

In order to distribute API processing and provide additional scalability both for updating APIs and serving DNS and DHCP protocols, Cloud Network Automation enables you to delegate specific sets of IPAM, DNS, and DHCP data to one or more Cloud Platform Appliances. Once authority for an object or set of objects has been delegated to a Cloud Platform Appliance, cloud API requests to create, modify, or delete objects under the scope of delegation for that appliance are processed locally and immediately available for serving DNS and DHCP to VMs within the cloud. This eliminates the need to send requests to the Grid Master to create, modify, or delete objects within the Grid. Changes made to objects on individual Cloud Platform Appliances are synchronized with the Grid Master in near real time using Grid replication to provide centralized visibility while retaining distributed processing capability. If a Cloud Platform Appliance is not authoritative for the object referenced in the cloud API requests, it automatically proxies that request to the Cloud Platform Appliance that is authoritative for the object or to the Grid Master (if it is authoritative for the object). Similarly, cloud API requests made to the Grid Master are proxied to the authoritative Cloud Platform Appliance or processed locally on the Grid Master if it is authoritative for the object. For information about authority delegation for supported objects, see **About Authority Delegation**. For information about proxying cloud API requests, see **Proxying Cloud API Requests**.

Cloud API requests are processed through the cloud API service that operates on the Cloud Platform Appliance. This service can also be enabled on the Grid Master as well as other Cloud Platform Appliances. The cloud API service is HTTPS-based; therefore, to ensure that the cloud API service functions properly, port 443 for HTTPS connectivity must be open between the CMP and each Cloud Platform Appliance and/or the Grid Master receiving the cloud API requests. To ensure that the proxying function works properly, port 443 for HTTPS must be open bi-directionally between each of the Cloud Platform Appliances as well as between each Cloud Platform Appliance and the Grid Master. You must also configure your firewalls and ACLs accordingly. Note that this service uses the VIP address on each Infoblox appliance as the destination address.

All objects created, modified, or deleted by the cloud adapter are reflected in the NIOS database. You can view cloud objects and their associated data in the **Cloud** tab of Grid Manager if the Cloud Network Automation license is installed on the Grid Master. For more information, see **Viewing Cloud Objects**. Note that it is possible to use Cloud Platform Appliances without deploying the Cloud Network Automation license. However, without the Cloud Network Automation license, VM and tenant information is only displayed as extensible attributes associated with IPAM, DHCP, and DNS objects in Grid Manager rather than in separate tables under the **Cloud** Tab.

Before you can send cloud API requests to a Cloud Platform Appliance or the Grid Master, you must create admin groups that have cloud API access. Only admin users that have cloud API access and applicable permissions may be used for sending cloud API requests. If the Cloud Network Automation license is installed on the Grid Master, it is also possible to assign **Tenant** permissions to admin users to restrict these users to only be able to view objects related to a given tenant or a set of tenants. For information about admin groups and how to manage admin users, see **Managing Administrators**.

Note: Unlike standard WAPI requests, all cloud API related events are logged to the NIOS syslog instead of the NIOS audit log.

---

**Figure 7.1 Cloud Network Automation**
Licensing Requirements

To enable Cloud Network Automation, you must install valid licenses on the Grid Master and Cloud Platform Appliance members. Depending on your deployment scenarios, you can take advantage of Elastic Scaling to automatically deploy virtual cloud appliances, either inside or outside your CMP. For more information about Elastic Scaling and how to use it, see the table below provides information about the IB-FLEX platform and various flavor settings.

The table below provides information about the IB-FLEX platform and various flavor settings.

| Cloud Network Automation license on the Grid Master and Grid Master Candidate |
| Cloud Platform license on the Cloud Platform Appliances |

The following valid licenses are part of the Cloud Network Automation solution:

- Cloud Network Automation license on the Grid Master and Grid Master Candidate
- Cloud Platform license on the Cloud Platform Appliances

The license you install on the Grid Master enables the Cloud user interface functions in Grid Manager and Tenant permissions.

The license you install on the Cloud Platform Appliance enables the cloud API service on the Cloud Platform Appliance.

Note that it is possible to use the Cloud Network Automation solution only with the Cloud Network Automation license or with one or more Cloud Platform Appliances. In the case when only the Cloud Network Automation license is installed on the Grid Master, all cloud API requests are sent to the Grid Master instead of to individual Grid members. Creation of cloud objects through cloud API requests is visible in the Cloud tab of Grid Manager on the Grid Master.

When Cloud Platform Appliances are used without the Cloud Network Automation license, cloud API requests are sent either to the Cloud Platform Appliances or to the Grid Master. However, the Cloud tab in Grid Manager is not available on the Grid Master for viewing cloud objects created through cloud API requests.

You can also use the CLI command set temp_license to generate and install temporary licenses. This provides licensed features and functionality for the interim, while you wait for your permanent licenses to arrive. For information about how to install a temporary license, see Adding Temporarily Licenses. Note that the temporary license is only effective on the Grid Master, not the Grid Master Candidate.

For an HA pair, ensure that you use the same appliance models for both nodes and install the Cloud Platform license on both nodes as well. For information about supported models, see Supported Cloud Platform Appliance Models. If a failover occurs and the passive node does not have a valid license, the cloud API service will stop and all resource delegations to the Cloud Platform Appliance will also stop.

Note that the Cloud Network Automation license on the Grid Master is incompatible with the following licenses:

- Multi-Grid Manager
- Reporting

Cloud Platform licenses are only supported on Cloud Platform Appliances. They may not be installed on any other Infoblox physical or virtual appliances. The following licenses and functionality are not supported on the Cloud Platform Appliances:

- Microsoft Management
- Multi-Grid Management
- Network Insight
- Reporting
- Tiered DNS Cache Acceleration
- DNS Cache Acceleration
- Load Balancing
- Infoblox
- RIR (Regional Internet Registry)
Before you install or remove the Cloud Platform license, consider the following:

- Installing or removing the Cloud Platform license stops the cloud API service.
- When you remove the Cloud Platform license from the appliance, it still serves DNS and DHCP if those licenses are installed on the appliance. However, the appliance will no longer be able to run the cloud API service. In addition, you cannot delegate authority to this member for objects that have not already been delegated to this appliance. Existing delegations to this member remain in the NIOS database, but API requests proxied from other Cloud Platform Appliances or from the Grid Master will fail.

**Licensing Configurations**

Depending on your Grid configuration and how you want to deploy Cloud Network Automation, Infoblox supports the following licensing configurations. For information about cloud licenses and how to install them, see [Licensing Requirements](#).

- **In an Infoblox Grid, the Grid Master has the Cloud Network Automation license installed and the Cloud Platform Appliance has the Cloud Platform license installed**: The Grid Master can process both regular RESTful API and cloud API requests and the Cloud Platform Appliance can process cloud API requests. With the Cloud Platform license installed, cloud API requests can be proxied among the Grid Master and Cloud Network Appliances based on the delegation authority of the referenced objects. You can also manage the cloud API service and cloud objects through the Cloud tab in Grid Manager.
- **In an Infoblox Grid, the Grid Master does not have the Cloud Network Automation license installed but the Cloud Platform Appliance has the Cloud Platform license installed**: The Grid Master can process both regular RESTful API and cloud API requests and the Cloud Platform Appliance can process cloud API requests. With the Cloud Platform license installed, cloud API requests can be proxied among the Grid Master and Grid Network Appliances based on the authority delegation of the referenced objects. Without the Cloud Network Automation license however, only objects whose authority has been delegated to Cloud Platform Appliances can be managed through Grid Manager. You will not have visibility of cloud objects, such as tenant information, through Grid Manager because the Cloud user interface function (the Cloud tab) is not available without the Cloud Network Automation license. You may manage cloud objects and their respective data through cloud API requests.
- **In an Infoblox Grid with other Grid members but without Cloud Platform Appliances, the Grid Master has the Cloud Network Automation license installed**: The Grid Master can process both regular RESTful API and cloud API requests. You can also manage cloud objects through the Cloud tab in Grid Manager.
- **Standalone Grid Master with the Cloud Network Automation license installed**: The appliance can process both regular RESTful API and cloud API requests. You can also manage the cloud API service and cloud objects through the Cloud tab in Grid Manager.
- **Standalone Grid Master without the Cloud Network Automation license installed**: The appliance can process only regular RESTful API requests, but not cloud API requests. You cannot manage the cloud API service nor cloud objects through Grid Manager because the Cloud user interface function (the Cloud tab) is not available.

The following table summarizes the supported licensing scenarios:

<table>
<thead>
<tr>
<th>Infoblox Grid with Cloud Platform Appliance(s)</th>
<th>Cloud Network Automation License on Grid Master</th>
<th>Cloud Platform License on Cloud Platform Appliance</th>
<th>Supports Regular RESTful API Calls on Grid Master</th>
<th>Supports Cloud API Calls on Grid Master and/or Cloud Platform Appliance(s)</th>
<th>Cloud User Interface Function in Grid Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infoblox Grid with Cloud Platform Appliance(s)</strong></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Infoblox Grid with Cloud Platform Appliance(s)</strong></td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Infoblox Grid with other Grid members but without Cloud Platform Appliance(s)</strong></td>
<td>✓</td>
<td>N/A</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Standalone Grid Master</strong></td>
<td>✓</td>
<td>N/A</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Standalone Grid Master</strong></td>
<td>✗</td>
<td>N/A</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>

**Administrative Permissions**

You must define admin users and their permissions in the admin group and assign specific roles to it before you can use these admin users to send cloud API requests. You can also define object permissions to specific admin groups or admin users so they can manage specific objects through cloud API requests. For more information, see [About Admin Accounts](#) and [About Admin Groups](#).

**Note**: When you deploy Cloud Network Automation, the *cloud-api-only* is created automatically. You cannot delete this admin group.

Depending on where a cloud API request is sent and whether the scope of delegation for an object is explicit or implicit, permissions configured for the admin user and object may or may not apply. In addition, depending on the objects referenced in cloud API requests, specific restrictions may apply. For supported objects and their restrictions, see [Supported Cloud API Objects](#).

For cloud API requests, admin permissions are applied based on the delegation status of the objects referenced in the requests. If an object is not...
delegated (owned by the Grid Master) and the cloud API request is sent directly to the Grid Master or proxied to the Grid Master, all applicable admin and object permissions apply. On the other hand, if authority for an object referenced in a cloud API request is explicitly delegated to a Cloud Platform Appliance and the request is sent to this appliance, the admin user has full permission for this object within the scope of delegation. In this case, specific permissions configured for the admin user and the referenced object are ignored. For more information about admin and object permissions, see About Administrative Permissions.

It is important to note that once you delegate authority of an object to the Cloud Platform Appliance, specific admin and object permissions are not enforced. Therefore, if you do not want certain objects to be created or modified through a cloud API request, do not delegate the authority of these objects and their parent objects to a Cloud Platform Appliance. For example, if you do not want host records to be created through cloud API requests, do not delegate the authority of the relevant networks, zones, or both to the Cloud Platform Appliance. On the other hand, if you want the ability to restrict permissions for specific objects referenced in cloud API updates, you can create different admin groups or admin users that are authorized to make cloud API updates on respective Cloud Platform Appliances. The following example illustrates this capability.

Configuration Example

If you want to restrict the creation and modification of records for networks 10.10.10.0/24 and 10.10.20.0/24 through cloud API updates, do the following:

1. Create two admin users APIUser1 and APIUser2 in an admin group.
2. Delegate the authority of network 10.10.10.0/24 to Cloud Platform Appliance 1 (CP1) and 10.10.20.0/24 to Cloud Platform Appliance 2 (CP2).
3. On CP1, add APIUser1 and on CP2, add APIUser2 to the list of administrators that can send cloud API requests, as described in Configuring Grid and Member Cloud API Properties.

Now when you use APIUser1 to send cloud API requests, you can add and modify records for network 10.10.10.0/24, but you cannot do so for network 10.10.20.0/24. Conversely, you can add and modify records for network 10.10.20.0/24 only when you use APIUser2.

Supported Cloud Platform Appliance Models

The following table lists the Infoblox vNIOS virtual appliances that you can use as Cloud Platform Appliances. A Cloud Platform Appliance can only be configured as a Grid member, not a standalone appliance. To configure an HA pair, you must use the same vNIOS models for both the active and passive nodes. For information about HA pairs, see About HA Pairs.

**Note:** Cloud Platform Appliances do not support auto-provisioning. Pre-provisioning is supported for DNS and DHCP data. For information about pre-provisioning Cloud Platform Appliances, see Pre-Provisioning NIOS and vNIOS Appliances.

<table>
<thead>
<tr>
<th>vNIOS Appliance</th>
<th>Storage (GB)</th>
<th># of CPU Cores</th>
<th>Virtual CPU Core Frequency</th>
<th>Memory Allocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-V800</td>
<td>160</td>
<td>2</td>
<td>2000 MHz</td>
<td>2 GB</td>
</tr>
<tr>
<td>CP-V1400</td>
<td>160</td>
<td>4</td>
<td>6000 MHz</td>
<td>8 GB</td>
</tr>
<tr>
<td>CP-V2200</td>
<td>160</td>
<td>4</td>
<td>12000 MHz</td>
<td>12 GB</td>
</tr>
</tbody>
</table>

Setting Up Cloud Network Automation

To set up Cloud Network Automation, ensure that you understand the required components, licenses, and firewall configuration, as described in Cloud Network Automation Operations. You also need to understand what a Grid is and how to set up a Grid and deploy vNIOS appliances. For more information, see Introduction to Grids.

Following are high-level steps for setting up Cloud Network Automation:

1. Evaluate your network topology and IPAM requirements, and then decide how you want to set up your Grid in the cloud environment. Based on your requirements, install and configure a cloud adapter that supports Cloud Platform Appliances on your CMP. This adapter functions as the cloud API client. For information about how to install and configure the cloud adapter, refer to the Quick Start Guide for the cloud adapter you are deploying, available on the Infoblox Support site. If you are implementing Cloud Network Automation in your Amazon VPCs (Virtual Private Clouds), refer to the Infoblox Installation Guide for vNIOS for AWS.
2. Obtain valid licenses through your Infoblox representatives. Note that Cloud Platform licenses may only be installed on cloud virtual appliances. They may not be installed on physical or virtual Trinzic Enterprise appliances. Deploy the Cloud Platform Appliances and install the Cloud Platform license along with the Enterprise, vNIOS, DHCP, and DNS licenses included in the license bundle for the Cloud Platform Appliance. If you plan to use the Cloud user interface functionality on the Grid Master, obtain a Cloud Network Automation license for your Grid Master and Grid Master Candidate. For information about how to obtain and install licenses, see Managing Licenses.

If you are implementing Cloud Network Automation in AWS, consider Elastic Scaling to see if it better fits your business needs when you purchase your licenses. You can purchase multiple dynamic licenses and automatically pre-provision vNIOS cloud appliances according to your business needs. For information about Elastic Scaling, see The table below provides information about the IB-FLEX platform and various flavor settings.

1. If the Cloud Platform Appliance is not part of the Grid, join it to the Grid. For more information about how to join a member to the Grid, see Joining Appliances to the Grid. If you have implemented Elastic Scaling, ensure that you follow the necessary steps to automatically

Copyright ©2019, Infoblox, Inc. All right reserved.
provision your vNIOS cloud appliances and join them to the Grid. For more information, see Using Elastic Scaling to Pre-provision and Launch vNIOS Members.

2. Log in to Grid Manager and complete the following:
   • Start the cloud API service on the Cloud Platform Appliance, as described in Starting the Cloud API Service

   The cloud API service is disabled by default.
   • Define admin groups and admin permissions for Cloud Network Automation, as described in About Admin Accounts and About Admin Groups.
   • Control which users can send API requests, as described in Configuring Grid and Member Cloud API Properties.
   • Add global and object permissions for admin users who can manage cloud objects, as described in Managing Permissions.

You can now start sending API requests through the cloud adapter or AWS API Proxy. To understand the API request process and the supported API objects, see About Cloud API Requests.

About Cloud API Service

The cloud API service provides the ability to automate management of IP addresses and DNS records so your cloud environment can take full advantage of IPAM, DNS, and DHCP capabilities in NIOS without the need for manual intervention. This service is supported for the following scenarios:

• Communication between the cloud adapter (acting as an API client) and the Cloud Platform Appliance or between Cloud Platform Appliances. This cloud API service accepts and processes a subset of the WAPI requests that are currently supported on the Grid Master either directly from an adapter or proxied through another Cloud Platform Appliance or from the Grid Master.
• Communication between the cloud adapter and the Grid Master, or between Cloud Platform Appliances and the Grid Master. This cloud API service processes requests received directly from the cloud adapter or processes requests received by other Cloud Platform Grid members.

The admin users that you use to send cloud API requests must have applicable access to the cloud API in order for the API requests to be processed. For information about admin groups, see Managing Admin Groups and Admin Roles.

Starting the Cloud API Service

To start the cloud API Service:

1. From the Grid tab, select the Services tab -> cloud_member check box.
2. Click Cloud API on the top navigation bar, and then click Start from the Toolbar.

Monitoring Cloud API Service

To monitor the status of the cloud API service, from the Cloud tab, select the Members tab -> cloud_member link. Grid Manager displays the service status, as described in Service Status.

You can also monitor the cloud API service through the following:

• View the cloud API service through the Member service status, as described in Member Status.
• Configure the appliance to receive SNMP traps for the cloud API service, as described in Monitoring with SNMP.
• View Cloud Statistics widget on the Dashboard, as described in Cloud Statistics.
• Review event messages in the syslog, as described in Viewing the Syslog.

About Cloud API Requests

In your cloud environment, the cloud adapter acts as the cloud API client. Only API requests made by admin users who have the correct permissions on the cloud API ACL (Access Control List) are processed by the cloud API service. When the Cloud Platform Appliance receives a cloud API request, it processes the request based on authority delegation of the objects and respective cloud extensible attributes. For information about cloud extensible attributes, see Extensible Attributes for Cloud Objects. If the Cloud Platform Appliance is not authoritative for the referenced objects, it proxies the request to the authoritative appliance that can be another Cloud Platform Appliance or to the Grid Master if no authority delegation is defined. For information about proxying cloud API requests, see Proxying Cloud API Requests.

Note: For the cloud API service to function properly, configure your networks and firewalls accordingly to allow port 443 HTTPS connectivity between the cloud adapter and Cloud Platform Appliance, between the cloud adapter and the Grid Master (if applicable), between the Grid Master and Cloud Platform members, and between each Cloud Platform member.

If you are using the AWS API Proxy to send API requests, ensure that you understand how to set up and configure the proxy. For detailed information, refer to the Infoblox Installation Guide for vNIOS for AWS.

When implementing Cloud Network Automation in AWS, you can use Elastic Scaling to allocate and deallocate dynamic licenses and automatically spin up vNIOS Grid members and join them to the Grid. You can purchase and install NIOS feature licenses in advance and store them in a license pool container on the Grid Master. You can then decide when and how to automatically provision and configure vNIOS for AWS cloud virtual appliances. When you remove a vNIOS cloud appliance, the licenses on this appliance are released and returned to the license pool and are available for the next deployment. For more information about Elastic Scaling, see The table below provides information about the IB-FLE X platform and various flavor settings.
## Cloud API Request Process

As described in Table 7.2, all cloud API requests are subject to the following process before responses are returned. The appliance

Table 7.2 Cloud API Request Process

<table>
<thead>
<tr>
<th>Steps</th>
<th>Descriptions</th>
<th>Configuration that affects the outcome of this step</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and categorization</td>
<td>All cloud API requests are authenticated based on the authentication sources. Once authenticated, the requests are categorized as either a cloud API request or not. All requests that specify user identity as users defined in admin groups with cloud API access are categorized as cloud API requests.</td>
<td>Define admin user accounts that can be used to send cloud API requests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For information, see Managing Admin Groups and Admin Roles.</td>
</tr>
<tr>
<td>Authorization</td>
<td>All cloud API requests are subject to authorization based on the ACLs (Access Control Lists) defined for the Grid or Cloud Platform Appliance. You can control which admin accounts can be used to send API requests. The ACLs can contain admin users in admin groups with cloud API access or remote authenticated users.</td>
<td>Define ACLs on the Grid Master or Cloud Platform Appliance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For information, see Configuring Grid and Member Cloud API Properties.</td>
</tr>
<tr>
<td>Proxying Requests</td>
<td>If a Cloud Platform Appliance is not authoritative for a cloud API request, it proxies the request either to the authoritative Cloud Platform Appliance or to the Grid Master for processing. Similarly, if an object has been delegated and the API request is made to the Grid Master, the Grid Master proxies that request to the authoritative Cloud Platform Appliance.</td>
<td>Ensure that HTTPS connectivity between each Cloud Platform member and between each Cloud Platform member and the Grid Master is functioning properly for proxying.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For information, see Proxying Cloud API Requests.</td>
</tr>
<tr>
<td>Validation</td>
<td>NIOS performs a final validation on the cloud API request based on permissions configured for the admin users and restrictions for the applicable objects. If the request is processed within the scope of an explicit delegation, the admin user is considered to have full permissions within the scope, and any permission defined for admin groups with cloud API access is ignored. Otherwise, the request is subject to validation for all permissions defined for admin groups with cloud API access.</td>
<td>Define admin permissions for admin groups with cloud API access.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For information, see About Admin Groups.</td>
</tr>
<tr>
<td>Auditing</td>
<td>Cloud API related events are logged to the NIOS syslog of the Grid member that processes the API requests instead of to the NIOS audit log.</td>
<td>Configure syslog server for the cloud member.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For information, see Viewing the Syslog.</td>
</tr>
</tbody>
</table>

## Supported Cloud API Objects

Table 7.3 lists all the supported cloud API object types, methods, and functions. In your cloud API requests, you cannot include RESTful API object types, methods, and functions that are not listed in the table, even when the Grid Master supports them for other purposes. Note that the supported types and operations for cloud API requests are sub sets of all types and operations supported on the Grid Master. Before you send any cloud API requests, ensure that you understand the implications and restrictions for each supported object. NIOS uses extensible attributes to associate specific information with a cloud object. For information about the default cloud extensible attributes and how to use them, see Extensible Attributes for Cloud Objects.

In AWS (Amazon Web Services), you can create a VPC (Virtual Private Cloud) and a subnet using the same network address and subnet mask. For example, you can add 172.29.02.0/24 as the VPC and 172.29.2.0/24 as the subnet and create VMs in the subnet. However, you cannot add a network container and a network using the same network address and subnet mask in NIOS. Therefore, when you send an API request to create such VPC and subnet in AWS, NIOS recognizes only the VPC, not the subnet. As a result, you are not able to create VMs under the subnet. For more information about how to create VPCs and subnets in AWS for NIOS, refer to the Infoblox Installation Guide for vNIOS for AWS.

In addition, when you delegate authority for supported cloud objects, NIOS may process the requests differently based on the following:

- How the object was first created.
- Whether authority for the object has already been delegated to a Cloud Platform Appliance.

For details about authority delegation and restrictions for each object, see About Authority Delegation.

**Note:** NIOS does not process cloud API requests that contain unsupported object types or any combination of supported object types with unsupported methods and functions. Although you can use all the fields in a supported object type, some restrictions may apply to supported values for some of these fields. For restrictions, see the Comments field in Table 7.3 for the corresponding object.
**Table 7.3 Supported Cloud API Objects for Cloud API Service**

*Note:* The cloud API service does not support scheduling and workflow approval requests. Objects deleted through a cloud API request are not stored in the Recycle Bin, except for DNS zones and network views. For information about the Recycle Bin, see *Using the Recycle Bin*.

<table>
<thead>
<tr>
<th>Supported Object Type</th>
<th>Cloud API Object</th>
<th>Allowed Operations in cloud API Requests</th>
<th>Authority Delegation and Restrictions</th>
<th>Required Extensible Attributes in cloud API Requests (for creations only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network View</td>
<td>networkview</td>
<td>Read, Create, Modify, Delete</td>
<td>See Network Views for information about authority delegation.</td>
<td>Tenant ID Cloud API Owned CMP Type</td>
</tr>
<tr>
<td>IPv4 Network Container</td>
<td>networkcontainer</td>
<td>Read, Create, Modify, Delete Function: next_available_network</td>
<td>Split network, join networks, and RIR related operations are not supported. See IPv4 and IPv6 Networks and Network Containers for information about authority delegation.</td>
<td>Tenant ID Cloud API Owned CMP Type</td>
</tr>
<tr>
<td>IPv6 Network Container</td>
<td>ipv6networkcontainer</td>
<td>Read, Create, Modify, Delete Function: next_available_network</td>
<td>Split network, join networks, and RIR related operations are not supported. See IPv4 and IPv6 Networks and Network Containers for information about authority delegation.</td>
<td>Tenant ID Cloud API Owned CMP Type</td>
</tr>
<tr>
<td>IPv4 Network</td>
<td>network</td>
<td>Read, Create, Modify, Delete Function: next_available_ip</td>
<td>Split network, join networks, and RIR related operations are not supported. See IPv4 and IPv6 Networks and Network Containers for information about authority delegation.</td>
<td>Tenant ID Cloud API Owned CMP Type</td>
</tr>
<tr>
<td>IPv6 Network</td>
<td>ipv6network</td>
<td>Read, Create, Modify, Delete Function: next_available_ip</td>
<td>Split network, join networks, and RIR related operations are not supported. See IPv4 and IPv6 Networks and Network Containers for information about authority delegation.</td>
<td>Tenant ID Cloud API Owned CMP Type</td>
</tr>
<tr>
<td>IPv4 DHCP Range</td>
<td>range</td>
<td>Read, Create, Modify, Delete Function: next_available_ip</td>
<td>See DHCP Ranges for information about authority delegation.</td>
<td>Tenant ID Cloud API Owned CMP Type</td>
</tr>
<tr>
<td>IPv6 DHCP Range</td>
<td>ipv6range</td>
<td>Read, Create, Modify, Delete Function: next_available_ip</td>
<td>See DHCP Ranges for information about authority delegation.</td>
<td>Tenant ID Cloud API Owned CMP Type</td>
</tr>
<tr>
<td>IPv4 Fixed Address (Reservation)</td>
<td>fixedaddress</td>
<td>Read, Create, Modify, Delete Function: next_available_ip You can also create and delete through Grid Manager. All required Cloud EAs are automatically populated in the GUI.</td>
<td>See IPv4 and IPv6 Fixed Addresses for information about authority delegation.</td>
<td>Tenant ID Cloud API Owned CMP Type</td>
</tr>
<tr>
<td>IPv6 Fixed Address (Reservation)</td>
<td>ipv6fixedaddress</td>
<td>Read, Create, Modify, Delete Function: next_available_ip You can also create and delete through Grid Manager. All required Cloud EAs are automatically populated in the GUI.</td>
<td>See IPv4 and IPv6 Fixed Addresses for information about authority delegation.</td>
<td>Tenant ID Cloud API Owned CMP Type</td>
</tr>
<tr>
<td>DNS View</td>
<td>view</td>
<td>Read, Modify</td>
<td>See <a href="#">DNS Views</a> for information about authority delegation.</td>
<td>Tenant ID</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>DNS Zone</td>
<td>zone_auth</td>
<td>Read, Create, Modify, Delete</td>
<td>See <a href="#">DNS Zones</a> for information about authority delegation.</td>
<td>Tenant ID</td>
</tr>
<tr>
<td>Host Record</td>
<td>record:host</td>
<td>Read, Create, Modify, Delete</td>
<td>You can also create and delete through Grid Manager. All required Cloud EAs are automatically populated in the GUI.</td>
<td>Tenant ID</td>
</tr>
<tr>
<td></td>
<td>record:host_ipv4addr</td>
<td>Read, Create, Modify, Delete</td>
<td>Function: next_available_ip</td>
<td>You can also create and delete through Grid Manager. All required Cloud EAs are automatically populated in the GUI.</td>
</tr>
<tr>
<td></td>
<td>record:host_ipv6addr</td>
<td>Read, Create, Modify, Delete</td>
<td>Function: next_available_ip</td>
<td>You can also create and delete through Grid Manager. All required Cloud EAs are automatically populated in the GUI.</td>
</tr>
<tr>
<td>Resource Record</td>
<td>record:a</td>
<td>Read, Create, Modify, Delete</td>
<td>Function: next_available_ip</td>
<td>See <a href="#">DNS Resource Records</a> or information about authority delegation.</td>
</tr>
<tr>
<td></td>
<td>record:aaaa</td>
<td>Read, Create, Modify, Delete</td>
<td>Function: next_available_ip</td>
<td></td>
</tr>
<tr>
<td></td>
<td>record:cname</td>
<td>Read, Create, Modify, Delete</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>record:ptr</td>
<td>Read, Create, Modify, Delete</td>
<td>Function: next_available_ip</td>
<td></td>
</tr>
<tr>
<td></td>
<td>record:mx</td>
<td>Read, Create, Modify, Delete</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>record:naptr</td>
<td>Read, Create, Modify, Delete</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>record:_srv</td>
<td>Read, Create, Modify, Delete</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>record:txt</td>
<td>Read, Create, Modify, Delete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grid Member</td>
<td>member</td>
<td>Read only</td>
<td>API requests calling for service restarts on a Grid member can be processed by the Cloud Platform Appliance only if the member requested is also the Cloud Platform Appliance processing the request.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Function: restartservices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grid</td>
<td>grid</td>
<td>Read only</td>
<td>All cloud API requests calling for service restarts are proxied to the Grid Master.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Function: restartservices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extensible Attribute</td>
<td>extensibleattributedef</td>
<td>Read only</td>
<td>You can use cloud attributes as source objects to obtain the next available IP address or network. When doing so, you must also include the respective network view for the object.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Proxying Cloud API Requests

In Cloud Network Automation, the primary Cloud Platform Appliance that receives cloud API requests can act as a proxy for other authoritative Cloud Platform members and for the Grid Master. This proxying mechanism is important when the Cloud Platform Appliance cannot process requests that contain objects for which it is not authoritative, or when objects in the requests do not have authority delegation and must be processed by the Grid Master.

Note that only successfully authenticated and authorized requests that require proxying are sent to the respective appliance for processing. Proxying is limited to one hop within the Grid. Therefore, if the destination appliance cannot process a proxied request, the request will not be forwarded and an error is returned to the client.

Note: Only cloud API requests can be proxied.

To ensure that the proxying mechanism functions properly, configure your systems to allow for the following communication:

- Allow all HTTPS connectivity among the Cloud Platform Appliances as well as to the Grid Master based on your organization's firewall requirements.
- Ensure that you use the VIP or the MGMT address if it is enabled (including that for the Grid Master) as the destination IP for the HTTPS connectivity. Note that this is a per member setting.
- Grant appropriate permissions to admin groups with cloud API access to ensure that tasks for objects outside of the delegation function properly on the Grid Master.

Sample Cloud API Requests

This section includes sample cloud API requests for supported objects:

Adding a network view:

```
curl -H "Content-Type: application/json" -k1 -u cloud:infoblox -X POST https://10.0.0.2/wapi/v2.0/networkview -d '{"name": "netview1", "extattrs": { "Tenant ID":{"value": "1011"},"Cloud API Owned":{"value":"True"},"CMP Type":{"value":"vCO/vCAC"}}}'
```

Adding a network within the delegated network view in the above example:

```
curl -H "Content-Type: application/json" -k1 -u cloud:infoblox -X POST https://10.0.0.2/wapi/v2.0/network -d '{ "network": "20.0.0.0/24", "network_view":"netview1","extattrs": { "Tenant ID":{"value": "1011"},"Cloud API Owned":{"value":"True"},"CMP Type":{"value":"vCO/vCAC"}}}'
```

Adding a DHCP range within the network created in the above example:

```
curl -H "Content-Type: application/json" -k1 -u cloud:infoblox -X POST https://10.0.0.2/wapi/v2.0/range -d '{ "end_addr": "20.0.0.40", "member": {"_struct": "dhcpmember1", "ipv4addr": "10.0.0.2", "name": "corpxyz.com"},"network": "20.0.0.0/24", "network_view": "netview1", "start_addr": "20.0.0.35", "extattrs": { "Tenant ID":{"value": "1011"},"CMP Type":{"value":"vCO/vCAC"},"Cloud API Owned":{"value":"True"}}}'
```

Adding an A Record:

```
curl -H "Content-Type: application/json" -k1 -u cloud:infoblox -X POST https://10.0.0.2/wapi/v2.0/record:a -d '{"name": "corp200.com", "ipv4addr":"20.0.0.2","view": "default.netview1","extattrs": { "Tenant ID":{"value": "1011"},"CMP Type":{"value":"vCO/vCAC"},"Cloud API Owned":{"value":"True"},"VM ID":{"value":"12"}}}'
```

Adding a Fixed address:

```
curl -H "Content-Type: application/json" -k1 -u cloud:infoblox -X POST https://10.0.0.2/wapi/v2.0/fixedaddress -d '{"ipv4addr": "20.0.0.5", "network_view": "netview1","mac":"15:06:32:16:00:00","extattrs": { "Tenant ID":{"value": "1011"},"CMP Type":{"value":"vCO/vCAC"},"VM ID":{"value":"352"},"Cloud API Owned":{"value":"True"}}}'
```

Adding a zone:

```
curl -H "Content-Type: application/json" -k1 -u cloud:infoblox -X POST https://10.0.0.2/wapi/v2.0/zone -auth-d '{"fqdn":"test.com","grid_primary": [{"name": "infoblox.localdomain", "stealth": false}],"name": "corpxyz.com", "stealth": false},"view": "default.netview1","extattrs": { "Tenant ID":{"value": "1011"},"CMP Type":{"value":"vCO/cCAC"},"Cloud API Owned":{"value":"True"}}}'
```

Adding a network container:

```
curl -H "Content-Type: application/json" -k1 -u cloud:infoblox -X POST https://10.0.0.2/wapi/v2.0/networkcontainer -d '{ "network": "200.0.0.0/24","network_view": "netview1","extattrs": { "Tenant ID":{"value": "1011"},"Cloud API Owned":{"value":"True"},"CMP Type":{"value":"vCO/vCAC"}}}'
```
Add a host record:

curl -H "Content-Type: application/json" -k -u cloud:infoblox -X POST https://10.0.0.2/wapi/v2.0/reco
dr:host -d '{ "ipv4addrs": [ { "configure_for_dhcp": false, "ipv4addr": "20.0.0.1", "mac": "11:22:22:22:33:33"} ], "ipv6addrs": [ { "configure_for_dhcp": false, "duid": "11:22", "ipv6addr": "13::1"} ], "name": "host.corpxyz.com", "view": "default.netview1" }'

Adding an MX Record:

curl -H "Content-Type: application/json" -k -u cloud:infoblox -X POST https://10.0.0.2/wapi/v2.0/reco
-d '{ "mail_exchanger": ", "name": ", "preference": 10, "view": "default.netview1", "extattrs": { "Tenant ID": { "value": "1011" }, "CMP Type": { "value": "vCO/vCAC" }, "Cloud API Owned": { "value": "False" }, "VM ID": { "value": "230" } } }'

Sample Cloud API Requests for Elastic Scaling

Creating a Member:

curl -H "Content-Type: application/json" -k -u cloud:cloud -X POST https://10.40.240.88/wapi/v2.2/mem
- d '{ "platform": "VNIOS", "host_name": "test1.com", "vip_setting": { "address": "1.1.1.1", "gateway": "1.1.0.2", "subnet_mask": "255.255.0.0" } }'

Getting a Member:

curl -H "Content-Type: application/json" -k -u cloud:cloud -X GET https://10.40.240.88/wapi/v2.2/memb

Adding Pre-Provisioned Information for the Member:

ber/b25lLnZpcnR1YWxfbm9kZSQ3:test1.com -d '{ "pre_provisioning": { "hardware_info": [ { "hwmodel": "CP-V1400", "hwtype": "IB-VNIOS" } ], "licenses": [ "cloud_api", "dhcp", "dns", "enterprise", "vnios" ] } }'

Creating and Delegating a Network View:

workview -d '{ "name": "testnv", "extattrs": { "Tenant ID": { "value": "1011" }, "CMP Type": { "value": "vm130ctest" }, "Cloud API Owned": { "value": "True" } } }'

Creating and Delegating a Network:

work -d '{ "network": "21.0.0.0/8", "network_view": "default", "cloud_info": { "delegated_member": { "ipv4addr": "1.1.1.1", "name": "test1.com" } }, "extattrs": { "Tenant ID": { "value": "1011" }, "CMP Type": { "value": "vm130ctest" }, "Cloud API Owned": { "value": "True" } } }'

Undelegating a Network:

curl -H "Content-Type: application/json" -k -u cloud:cloud -X PUT https://10.40.240.88/wapi/v2.2/network/ZG5zLm5ldHdvcmskMjEuMC4wLjAvOC8w:21.0.0.0/8/default -d '{ "cloud_info": { "delegated_member": null } }'

Creating and Delegating an Authoritative Zone

curl -H "Content-Type: application/json" -k -u cloud:cloud -X POST https://10.40.240.88/wapi/v2.2/zon
e_auth -d '{ "fqdn": "test.com", "grid_primary": [ { "name": "test1.com", "stealth": false } ], "view": "default", "extattrs": { "Tenant ID": { "value": "1011" }, "CMP Type": { "value": "vm130ctest" }, "Cloud API Owned": { "value": "True" } } }'

Deleting a Member:

curl -H "Content-Type: application/json" -k -u cloud:cloud -X DELETE https://10.40.240.88/wapi/v2.2/memb
ner/b25lLnZpcnR1YWxfbm9kZSQ3:test1.com

Creating Token for the Pre-Provisioned Member (note that only superuser can create a token; you must configure superusers admin groups with cloud API access):

curl -H "Content-Type: application/json" -k -u cloud:cloud -X POST https://10.40.240.88/wapi/v2.2/memb
ner/b25lLnZpcnR1YWxfbm9kZSQ3:test1.com?_function=create_token

Reading Token for the Pre-Provisioned Member (note that only superuser can create a token; you must configure superusers admin groups with cloud API access):

Copyright ©2019, Infoblox, Inc. All right reserved.

About Authority Delegation

Authority delegation in Cloud Network Automation is the ability to assign full and exclusive control of IP addresses and DNS name spaces to a Cloud Platform Appliance. You can perform authority delegation only through the Grid Master. When you delegate the authority of IP addresses and DNS name spaces to a Cloud Platform Appliance, the Grid Master loses its authority over the scope of delegation for these IP addresses and name spaces as well as any objects within them. Note that authority delegation for an object can be explicitly assigned or inherited from parent objects. For information about how to delegate authority for supported object types, see Guidelines for Delegating Authority.

About Authority Delegation

Authority delegation in Cloud Network Automation is the ability to assign full and exclusive control of IP addresses and DNS name spaces to a Cloud Platform Appliance. You can perform authority delegation only through the Grid Master. When you delegate the authority of IP addresses and DNS name spaces to a Cloud Platform Appliance, the Grid Master loses its authority over the scope of delegation for these IP addresses and name spaces as well as any objects within them. Note that authority delegation for an object can be explicitly assigned or inherited from parent objects. For information about how to delegate authority for supported object types, see Guidelines for Delegating Authority.

Note: You can delegate authority only to Cloud Platform Appliances, but not to other Grid members.

Objects that are in queue for scheduled executions or approvals are locked and cannot be delegated. Authority delegation and reclaiming of authority are subject to approval and can be scheduled.

Guidelines for Delegating Authority

You can initiate explicit delegation of authority only through Grid Manager on the Grid Master. The cloud API service can only be used for implicit or automatic delegation of an object such as creating a network under a network container that has been delegated, in which network is implicitly delegated to the member to which the network container is delegated.

The Grid Master can explicitly delegate authority only for the following object types:

- Network View
- Network Container (both IPv4 and IPv6)
- Network (both IPv4 and IPv6)
- DHCP Range (IPv4 and IPv6)
- DNS Authoritative Zone (Note that zones are implicitly delegated if the assigned name server is a Cloud Platform Appliance.)

Consider the following when you delegate authority for an object:

- You can delegate authority for supported objects to one and only one Cloud Platform Appliance, except for DNS zones.
- When delegating authority for a parent object, all child objects within the scope of delegation inherit the same authority delegation.
- You cannot delegate authority for the following:
  - objects whose parents already have a delegation configured
  - individual IPAM and DNS records including fixed addresses, host records, A/AAAA/PTR records, etc.
- When you use Elastic Scaling to pre-provision an offline Cloud Platform Appliance, any object authority delegated to this offline member does not take effect until the member joins the Grid. Therefore, you can still create child objects through Grid Manager under the delegated objects when the member is offline.
- You can override the inheritance of authority delegation at the object level only if the parent object has not been delegated. The Grid Master assumes authority for objects that do not fall within the scope of delegation.
- If a supported object has already been delegated, you cannot re-delegate it to another appliance. If you want to re-delegate this object, you must first un-delegate it.
- For explicitly delegated objects, you can only modify the permission and extensible attributes from Grid Manager and the Infoblox API other than cloud API requests. For explicitly delegated zones however, you can modify any properties from Grid Manager and the Infoblox API other than cloud API requests.
- When you create or delete a delegated object through a cloud API request, the appliance returns an OK message if the operation is successful. It returns an ERROR message if the operation fails. You can then change the options in the request and try again. The appliance sends a WARNING message when certain operations require attention.
- You can reclaim the authority that you delegated to a Cloud Platform Appliance. Once the authority is reclaimed, it goes back to the Grid Master. Before you reclaim authority for any object, ensure that the Cloud Platform Appliance is online and properly connected to the Grid Master for the reclaiming process to function properly.
- The Cloud Platform Appliance can run discovery on any network containers or networks that are reachable by the appliance. The default discovery settings for network containers and networks are inherited from their parent objects. For information about discovery, see About Discovery.

Note: Any Cloud Platform Appliances that are removed from the Grid automatically lose authority over objects that were delegated to them. The Grid Master becomes authoritative for these objects.

Delegating Authority for Cloud Objects

You can delegate authority when you create a new object that has not been delegated or does not inherit authority delegation from one of its parent objects. See the following sections for detailed information about delegating authority for supported objects.
Network Views

Consider the authority delegation guidelines in Table 7.4 when you create, modify, or delete a network view. See Sample Cloud API Requests for a sample cloud API request.
For information about how to create network views from the Grid Master, see Adding Network Views.

Table 7.4 Authority Delegation for Network Views

<table>
<thead>
<tr>
<th>Cloud API Requests</th>
<th>Standard API and WAPI Requests</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>• You can delegate authority for a network view to only one Cloud Platform Appliance.</td>
<td>• You can delete a network view from the Grid Master only if it has not been delegated to any Cloud Platform Appliance.</td>
<td>• When you create a network view through a cloud API request, you must include the following extensible attributes in the cloud API request: Tenant ID, Cloud API Owned, and CMP Type.</td>
</tr>
<tr>
<td>• When you create a new network view, authority is automatically delegated to the Cloud Platform Appliance that processes the request.</td>
<td>• When you create a network view on the Grid Master, it is shared among all Grid members in the Grid.</td>
<td></td>
</tr>
<tr>
<td>• To balance network views among multiple Cloud Platform Appliances in the Grid, ensure that you configure your cloud adapter accordingly.</td>
<td>• You can delegate a network view from the Grid Master to a Cloud Platform Appliance only if the child objects within the network view are delegated to the same Cloud Platform Appliance.</td>
<td></td>
</tr>
<tr>
<td>• If you want to share a network view among different Cloud Platform members, you must manually provision it and its child objects and delegate them to the respective Cloud Platform members.</td>
<td>• When you reclaim authority for a network view, any DNS zones in the network view remain assigned to their name servers, including the Cloud Platform Appliance that has lost authority over the network view. In other words, the DNS zone remains under the authority of that Cloud Platform Appliance.</td>
<td></td>
</tr>
</tbody>
</table>

IPv4 and IPv6 Networks and Network Containers

Consider the authority delegation guidelines in Table 7.5 when you create, modify, or delete a network or network container. See Sample Cloud API Requests for a sample cloud API request. For information about how to create IPv4 and IPv6 networks from the Grid Master, see Adding IPv4 Networks and Adding IPv6 Networks.
For information about how to create IPv4 and IPv6 networks using network templates from the Grid Master, see Adding IPv4 Network Templates and Adding IPv6 Network Templates.

Table 7.5 Authority Delegation for Networks and Network Containers

<table>
<thead>
<tr>
<th>Cloud API Requests</th>
<th>Standard API and WAPI Requests</th>
<th>Comments</th>
</tr>
</thead>
</table>

Copyright ©2019, Infoblox, Inc. All right reserved.
You can delegate authority for a network or network container to only one Cloud Platform Appliance, but you can delegate authority of multiple networks and network containers to the same Cloud Platform Appliance. When you create a new network or network container through a cloud API request, authority is automatically delegated to the primary Cloud Platform Appliance that processes the request. When you create a network using a network template, you must provide the name of the template and reference it in the cloud API request. Delegation for a network or network container (except for unmanaged networks) can be done through explicit delegation or inheritance from the parent object. You cannot delete networks and network containers using cloud API requests if they have already been explicitly delegated. You must first un-delegate them before deleting them. Networks and network containers associated with a DNS zone cannot be delegated. You can delegate a network or network container if all the following are true:

- It has not been delegated to a Cloud Platform Appliance.
- It is not part of a network or network container that has been delegated to a Cloud Platform Appliance.
- It does not contain any networks or DHCP ranges that are delegated to a different Cloud Platform Appliance.
- It does not belong to a delegated network view.
- All discovery related attributes for a network or network container return the default values.
- You cannot modify the discovery settings for networks that are in a delegated network container. You cannot create discovered networks in a network container whose authority has been delegated. You also cannot convert unmanaged networks. A discovered unmanaged IP address may co-exist with an IP address created through a cloud API request.
- Although no DHCP service restart is required, you can perform a DHCP service restart on a Cloud Platform Appliance through a cloud API request.

When you create a network or network container through a cloud API request, you must include the following extensible attributes in the request: Tenant ID, Cloud API Owned, and CMP Type. If a network is explicitly delegated (not through inheritance), you can convert a network to a network container only if the size of the network remains the same; the network delegation is transferred to the network container. The Cloud Platform Appliance does not support split network, join networks, and RIR related operations.

### DHCP Ranges

Consider the authority delegation guidelines in Table 7.6 when you create, modify, or delete a DHCP range. See Sample Cloud API Requests for a sample cloud API request. For information about how to create IPv4 and IPv6 ranges, see Adding IPv4 Address Ranges and Modifying IPv6 Address Ranges. For information about how to create IPv4 and IPv6 ranges using range templates, see Adding IPv4 Range Templates and Adding IPv6 Range Templates.

#### Table 7.6 Authority Delegation for DHCP Ranges

<table>
<thead>
<tr>
<th>Cloud API Requests</th>
<th>Standard API and WAPI Requests</th>
<th>Comments</th>
</tr>
</thead>
</table>

Copyright ©2019, Infoblox, Inc. All right reserved.
You can delegate authority for a DHCP range to only one Cloud Platform Appliance, but you can delegate authority for multiple DHCP ranges to the same Cloud Platform Appliance.

When you create a new DHCP range, authority is automatically delegated to the Cloud Platform Appliance that processes the request or to the Grid Master if the Grid Master processes the request.

When you create a DHCP range using a range template, you must know the name of the template and reference it in the cloud API request.

You can delegate authority for reserved ranges in a Microsoft synchronized network if:

- It is not included in any exclusions.
- It does not conflict with another reserved range.

You can manage these range addresses through a cloud adapter, such as the IPAM Plug-In for VMware.

Delegation for a DHCP range can be done through explicit delegation or inheritance from the parent object. You cannot override inherited delegation.

Note that you cannot delete DHCP ranges using cloud API requests if they have already been explicitly delegated. You must first un-delegate them before deleting them. However, if the delegation is inherited, you can delete the objects through a cloud API request.

You can delegate a DHCP range to a Cloud Platform Appliance if all the following are true:

- It has not been delegated to a Cloud Platform Appliance.
- It is not part of a delegated network or network container in the same network view.
- It does not belong to a delegated network view.
- It is a reserved range or a range that has been assigned to a DHCP member that is the same Cloud Platform Appliance to which you want to delegate the range.

You cannot delegate a DHCP range that has been assigned to a failover association, nor can you assign a DHCP range that has been delegated to a failover association.

Authority is delegated from the start address to the end address, including exclusions. Note that the exclusions can be used only to restrict IP addresses generated by the next available IP feature.

All discovery related attributes for a DHCP range return the default values.

Although no DHCP service restart is required, you can perform a DHCP service restart on a Cloud Platform Appliance through a cloud API request.

IPv4 and IPv6 Fixed Addresses

Consider the following authority delegation guidelines when you create, modify, or delete a fixed address:

- You can delegate authority for a fixed address only through inheritance from one of its parent objects, such as its associated network view, network container, network, or DHCP reserved range.
- When you create or modify an IPv4 or IPv6 fixed address, you must include the following extensible attributes in the cloud API request: Tenant ID, Cloud API Owned, and CMP Type.
- You can create a fixed address from the Grid Master using a fixed address template. Note that when you want to reference a template in the cloud API request, you must know the name of the template beforehand.
- When performing any operations on a Cloud Platform Appliance, all discovery related attributes for a fixed address return the default values.
- No DHCP service restart is required when performing any operations for a fixed address on the Cloud Platform Appliance unless automatic DHCP restart is disabled on the appliance. You can however perform a DHCP service restart on the Cloud Platform Appliance to which authority is delegated for a fixed address through a cloud API request.
- You can create, modify, or delete an IPv4 or IPv6 fixed address and reservation on the Grid Master through Grid Manager if the fixed address or reservation is within the scope of a network view, network container, network, or DHCP reserved range whose authority has been delegated to a Cloud Platform Appliance.

See Sample Cloud API Requests for a sample cloud API request.

For information about how to create IPv4 and IPv6 fixed addresses, see Adding IPv4 Fixed Addresses and Adding IPv6 Fixed Addresses.

For information about how to create IPv4 and IPv6 fixed address templates, see Adding IPv4 Fixed Address/Reservation Templates and Adding IPv6 Fixed Address Templates.

Copyright ©2019, Infoblox, Inc.All right reserved.
DNS Views

Consider the following authority delegation guidelines when you create, modify, or delete a DNS view:

- You cannot explicitly delegate authority for a DNS view. The Cloud Platform Appliance automatically gains authority over any DNS view that exists in the network view whose authority is delegated to that appliance.
- You cannot create or delete a DNS view from the Cloud Platform Appliance.
- Through a cloud API request, you can update DNS views defined in a network view that has been delegated to the Cloud Platform Appliance.
- You cannot create, modify, or delete a DNS view in network views that have been delegated to a Cloud Platform Appliance through a standard API request.
- You cannot delete a DNS view as long as it contains at least one DNS zone that has been delegated to a Cloud Platform Appliance.

DNS Zones

Consider the following authority delegation guidelines in Table 7.7 when you create, modify, or delete a DNS zone. See Sample Cloud API Requests for a sample cloud API request.

For information about how to create DNS zones, see About Authoritative Zones.

Table 7.7 Authority Delegation for DNS Zones

<table>
<thead>
<tr>
<th>Cloud API Requests</th>
<th>Standard API and WA PI Requests</th>
<th>Comments</th>
</tr>
</thead>
</table>
| • The Grid primary of a DNS zone automatically gains authority for the zone if the primary is a Cloud Platform Appliance. When there are multiple primaries configured for the zone, multiple delegations to these primaries are allowed as long as they are Cloud Platform Appliances.  
  • You cannot assign both a Microsoft server and a Grid member as primaries at the same time, although you can assign a Microsoft server as the Grid primary and a Cloud Platform Appliance as the Grid secondary. This allows the Microsoft server to serve changes sent from the cloud adapter.  
  • All resource records in a DNS zone inherit authority delegation from the zone. However, you cannot modify the NS record through a cloud API request.  
  • You can modify all the fields for a zone whose authority has been explicitly delegated.  
  • The cloud member to which authority for a network view is delegated automatically gains authority for authoritative zones defined in that network view. This Cloud Platform Appliance is the only cloud member that can be the Grid primary for the zones defined in this network view. The Grid Master does not have authority for any zone in this network view unless it is assigned as a Grid primary.  
  • The Cloud Platform Appliance can create, modify, and delete a DNS zone in any DNS view defined in a network view whose authority has been delegated to that cloud member.  
  • The Cloud Platform Appliance that is authoritative for a DNS zone can perform changes to the assigned Grid primaries, Grid secondaries, and external servers assigned to the zone as long as the Cloud Platform Appliance remains a Grid primary. But it cannot create, modify, or delete the NS record.  
  • The Cloud Platform Appliance that is authoritative for a DNS zone can create, modify, and delete DNS delegations that are directly parented to that zone. In particular, it may specify any Grid primary, Grid secondary, or external server for that zone.  
  • DNSSEC operations, network associations, and zone locking are not supported if at least one Cloud Platform Appliance is assigned as the Grid primary for any DNS zones.  
  • Although no DHCP service restart is required, you can perform a DHCP service restart on a Cloud Platform Appliance through a cloud API request. | • You cannot create, modify, or delete a DNS zone in a network view whose authority has been delegated to a Cloud Platform Appliance.  
  • You cannot assign a Cloud Platform Appliance as the Grid primary for a zone that is locked or disabled.  
  • You can modify extensible attributes of any DNS zone whose authority has been delegated from the Grid Master. | • Only authority for authoritative forward-mapping and reverse-mapping zones can be delegated. You cannot delegate authority for forward zones, stub zones, and delegated zones even though they may exist in a delegated network view.  
  • When you create a DNS zone using a cloud API request, you must include the following extensible attributes in the request: Tenant ID, Cloud API Owned, and CMP Type. |
DNS Resource Records

Consider the following authority delegation guidelines in Table 7.8 when you create, modify, or delete a resource record, including A, AAAA, CNAME, PTR, MX, SRV, TXT, NAPTR records. See Sample Cloud API Requests for a sample cloud API request.

Table 7.8 Authority Delegation for DNS Resource Records

<table>
<thead>
<tr>
<th>Cloud API Requests</th>
<th>Standard API and WAPI Requests</th>
<th>Comments</th>
</tr>
</thead>
</table>
| • Authority delegation for resource records (A, AAAA, CNAME, PTR, MX, SRV, TXT, and NAPTR) is inherited from their parent zones. You can delegate authority for these records by delegating authority for their respective parent zones.  
• All resource records in a DNS zone inherit authority delegation from their parent zones. However, you cannot modify the NS record through a cloud API request.  
• If the Cloud Platform Appliance is a Grid primary for a zone, requests that include a supported record is processed locally by the Cloud Platform Appliance. Otherwise, the request is proxied to the Cloud Platform Appliance that is assigned as the only Grid primary for the zone.  
• If the DNS resource records belong to a zone that is served only by Cloud Platform Appliances, authority for these records are considered delegated. You must create, modify, or delete these records on one of these Cloud Platform Appliances. | • You cannot create, modify, or delete a resource record if it is in a network view whose authority has been delegated to a Cloud Platform Appliance.  
• When you create a resource record through a cloud API request, you must include the following extensible attributes in the request: Tenant ID, Cloud API Owned, and CMP Type. | |

Host Records

Consider the following authority delegation guidelines in Table 7.9 when you create, modify, or delete a host record. See Sample Cloud API Requests for a sample cloud API request.

Table 7.9 Authority Delegation for Host Records

<table>
<thead>
<tr>
<th>Cloud API Requests</th>
<th>Standard API and WAPI Requests</th>
<th>Comments</th>
</tr>
</thead>
</table>
### Configuring Grid and Member Cloud API Properties

Only admin users in admin groups with cloud API access can be used to send cloud API queries by default. For information about how to add users to an admin group, see Creating Local Admins. To control which admin users, either from this group or from remote servers, can perform cloud API tasks, you can further define ACLs and member levels.

1. **Grid:** From the **Cloud** tab, click **Grid Cloud API Properties** from the Toolbar. Configuration done for the Grid only applies to the current Grid Master; it is not inherited by other Cloud Platform Appliances. Then complete the following:
   - **Member:** From the **Cloud** tab, select the **Members** tab -> member check box, and then click the Action icon 📝 and select **Edit** from the menu. Configuration done at the member level applies only to the Grid member.
2. In the **Grid Cloud API Properties** (for the current Grid Master) or the **Member Cloud API Properties** editor, select the **General** tab, and then complete the following:
   - **Administrator allowed to make WAPI request on the Grid Master**
     - **None:** When you select this, none of the admin users in admin groups with cloud API access can send cloud API requests to the Grid Master or Cloud Platform Appliance.
     - **All:** When you select this, all admin users in admin groups with cloud API access can send cloud API requests to the Grid Master or Cloud Platform Appliance. This is the default.
     - **Set of administrators:** Select this to create a list of admin users, both remote and local, who can send cloud API requests. Local users are users defined in admin groups with cloud API access. Remote users are users who log in from other remote servers. These users will be authenticated before they can access the Grid Master or Cloud Platform Appliance. To add local users, click the Add icon and select **Local**. In the **Cloud API Admin Selector**, select an admin user from the list. Grid Manager adds the selected user to the table. If you have only one cloud API user, Grid Manager automatically adds this user to the table.
     - To add remote users, click the Add icon and select **Remote**. Grid Manager adds a row to the table. Click the **Admin** column to add the username of the administrator. Note that the username you enter here must match the username used on the remote server. Depending on the remote server type, you must create a server group for these remote users and add the group to the admin authentication policy to ensure these admin users can send cloud API requests. For information about how to configure admin server groups and admin authentication policy, see About Remote Admins.
     - Click the Add icon again to add additional admin users.
   - **Recycle cloud objects:** This only applies to the Grid Master. Select this check box to enable the recycling of cloud objects. This is selected by default.
3. Save the configuration.

### Extensible Attributes for Cloud Objects

When you first enable Cloud Network Automation, NIOS installs a set of extensible attributes that are specific for cloud usage. Use these cloud extensible attributes to tag objects that belong to the CMP. Note the following when defining cloud extensible attributes through Grid Manager:

- Authority delegation for a host record is inherited from both the DNS and DHCP portions of the record. For DNS, you can delegate authority for all DNS zones for which the host record is defined. For DHCP, you can delegate authority for the parent network view, network container, network, or DHCP range defined for the host record.
- You can create, modify, or delete a host record or a host IP address whose authority is delegated to a Cloud Platform Appliance through Grid Manager. Note that when you create a host record, you must enable it for DNS within the delegated network view. Otherwise, you will not be able to save the host record.
- The Cloud Platform Appliance can process a cloud API request that includes a host record only if it has gained authority for both DNS and DHCP portions of the host record, as follows:
  - All IP addresses enabled for DHCP within one or more delegation scopes are delegated to the same Cloud Platform Appliance.
  - All DNS records defined for one or more DNS zones have the same Cloud Platform Appliance assigned as the Grid primary.
- IP addresses defined in the host record that is enabled for DHCP follow the same rules set for a fixed address. See IPv4 and IPv6 Fixed Addresses for more information.
- Names or aliases defined in the host record follow the same rules set for resource records. See DNS Resource Records for more information.
- Although no DHCP service restart is required, you can perform a DHCP service restart on a Cloud Platform Appliance through a cloud API request.
- When you create a host record through a cloud API request, you must include the following extensible attributes in the request: Tenant ID, Cloud API Owned, and CMP Type.
You cannot assign cloud extensible attributes to other NIOS objects, yet you can create smart folders using these cloud attributes or modify their definitions.

You can define and update cloud extensible attributes on the Grid Master, through cloud API requests or Grid Manager, as long as the authority for the corresponding cloud objects are not delegated.

To identify a cloud object, you must reference some of these cloud attributes when you create, modify, or delete a specific object. For more information about which extensible attributes are required for cloud API requests, see Supported Cloud API Objects.

5800255 lists the default cloud extensible attributes come installed on the appliance. Note that some of the attributes are read-only and you cannot modify their properties. These attributes are applicable for specific object types or for identification purposes. See Comments for more information about each attribute.

Note: All cloud extensible attributes are displayed in the Administration tab -> Extensible Attributes tab in Grid Manager.

### Table 7.10 Extensible Attributes for Cloud Usage

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>String</td>
<td>The CMP user account for creating networks.</td>
</tr>
<tr>
<td>Allocation ID</td>
<td>String</td>
<td>The allocation ID of the Elastic IP. Limited to Elastic IP only. Example: eipalloc-5723d13e.</td>
</tr>
<tr>
<td>Application Type</td>
<td>String</td>
<td>Indicates the application type, such as Web, DB, or CRM.</td>
</tr>
<tr>
<td>Association ID</td>
<td>String</td>
<td>Association ID specific to Elastic IP only.</td>
</tr>
<tr>
<td>Attachment ID</td>
<td>String</td>
<td>The attachment ID of the network interface. This is valid for Elastic IP only and present when Network Interface is attached to an instance. Example:eni-attach-d94b09b0.</td>
</tr>
<tr>
<td>Availability Zone</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>Cloud API Owned</td>
<td>List [True, False]</td>
<td>This is read-only. Defines whether an object was created by the cloud adapter.</td>
</tr>
<tr>
<td>Cloud Region</td>
<td>String</td>
<td>A region name for an VPC object. Example: us-west-1.</td>
</tr>
<tr>
<td>CMP Type</td>
<td>String</td>
<td>This is read-only. Defines the type of CMP, such as VMware or OpenStack.</td>
</tr>
<tr>
<td>Host Aggregates</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>Interface Name</td>
<td>String</td>
<td>The name of the interface.</td>
</tr>
<tr>
<td>Is External</td>
<td>List [True, False]</td>
<td>This is read-only. Limited to the object type Network and Network Container.</td>
</tr>
<tr>
<td>Is Primary Interface</td>
<td>List [True, False]</td>
<td>This is read-only.</td>
</tr>
<tr>
<td>Is Shared</td>
<td>List [True, False]</td>
<td>This is read-only. Limited to the object type Network and Network Container.</td>
</tr>
<tr>
<td>IP Type</td>
<td>List [Private, Public, Fixed, Floating, Elastic]</td>
<td>This is read-only. Type of IP address.</td>
</tr>
<tr>
<td>Location</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>Network Encap</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>Network ID</td>
<td>String</td>
<td>Network ID in OpenStack</td>
</tr>
<tr>
<td>Network Name</td>
<td>String</td>
<td>Network name</td>
</tr>
<tr>
<td>Physical Network Name</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>Port Attached Device - Device ID</td>
<td>String</td>
<td>Device ID for associated device, such as OpenStack or equivalent, in other CMPs.</td>
</tr>
<tr>
<td>Port Attached Device - Device Owner</td>
<td>String</td>
<td>Device name for associated device, such as OpenStack or equivalent, in other CMPs (e.g. compute:nova, network:dhcp, or netowrk:router_interface).</td>
</tr>
<tr>
<td>Port Group</td>
<td>String</td>
<td>VMware or equivalent in other Hypervisors or CMPs.</td>
</tr>
<tr>
<td>Port ID</td>
<td>String</td>
<td>Port ID for associated device, such as OpenStack or equivalent, in other CMPs.</td>
</tr>
<tr>
<td>Port Name</td>
<td>String</td>
<td>Port name for associated device, such as OpenStack or equivalent, in other CMPs.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Private IP</td>
<td>String</td>
<td>One or more secondary private IP addresses that are assigned to the given Network Interface.</td>
</tr>
<tr>
<td>Segmentation ID</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>Subnet ID</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>Subnet Name</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>Tenant ID</td>
<td>String</td>
<td>This is read-only. The unique ID for the tenant object.</td>
</tr>
<tr>
<td>vDC</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Integer</td>
<td>The VLAN ID.</td>
</tr>
<tr>
<td>VM ID</td>
<td>String</td>
<td>This is read-only. This is the Instance ID in OpenStack.</td>
</tr>
<tr>
<td>VM Name</td>
<td>String</td>
<td>Instance Name in OpenStack.</td>
</tr>
<tr>
<td>vCD App</td>
<td>String</td>
<td>The application name defined in vCloud Director; previously vApp</td>
</tr>
<tr>
<td>vCD Org</td>
<td>String</td>
<td>The organization name defined in vCloud Director; previously vOrg.</td>
</tr>
<tr>
<td>VPC ID</td>
<td>String</td>
<td>This is read-only. This is a naming convention that is used at the time of creation. Example: vpc-1a2b3c4d.</td>
</tr>
<tr>
<td>VPC Name</td>
<td>String</td>
<td>An optional name tag for the VPC.</td>
</tr>
<tr>
<td>VPCs List</td>
<td>String</td>
<td>List of all the VPCs.</td>
</tr>
</tbody>
</table>

You can modify some of the properties for the cloud extensible attributes, except for the read-only attributes. By default, all cloud extensible attributes are configured to allow Read/Write access for the Cloud Platform Appliances. You can change this configuration to read-only so the Cloud Platform Appliances can only access the attribute values, but not modify them. Note that when you reference modification for a read-only attribute in a cloud API request, the Cloud Platform Appliance returns an error because it cannot modify the attribute value. For information about how to configure extensible attributes, see About Extensible Attributes.

Note: An upgrade could fail if the name of an existing extensible attribute matches the name of any of the cloud extensible attribute for a different object type. You must define values for all required cloud extensible attributes in a cloud API request.

### Extensible Attributes for Tags in AWS and Azure

You can define metadata in the form of tags for AWS and Azure which are captured through a vDiscovery process and you can save the tags as extensible attributes in NIOS. You can use predefined attributes or create your own tags that consists of an user-defined key and an optional value. The tag values defined in AWS and Azure are translated into corresponding extensible attribute values in NIOS.

Note the following about saving tags defined in AWS and Azure as extensible attributes in NIOS:

- You must add extensible attributes in NIOS with the same name as the tags added in AWS or Azure.
- You can add or delete tags in Azure, but cannot update the tags.
- The tags are translated only when the corresponding extensible attributes are created in NIOS.
- The tags are discovered only during the next vDiscovery process after creating the corresponding extensible attributes in NIOS.
- It is not recommended to delete the extensible attributes which you have created for the tags defined in AWS and Azure.

The following table shows the translation of tags defined in AWS and Azure, as extensible attributes in NIOS:

<table>
<thead>
<tr>
<th>AWS Object</th>
<th>Azure Object</th>
<th>NIOS Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC-2 Instance</td>
<td>Virtual Machine</td>
<td>VM</td>
</tr>
<tr>
<td>Interface</td>
<td>Virtual Interface</td>
<td>Managed private IP address: Any DNS record, fixed address, or reservation associated with that IP address.</td>
</tr>
<tr>
<td>Interface (tags are the same for private IP address and public IP address of the same interface)</td>
<td>Public IP address (Public IP address has specific tags in Azure)</td>
<td>Managed public IP address: Any DNS record, fixed address, or reservation associated with the IP address.</td>
</tr>
<tr>
<td>VPC</td>
<td>Virtual Network</td>
<td>VPC</td>
</tr>
</tbody>
</table>
Viewing Cloud Objects

When you enable the Cloud Network Automation license on the Grid Master, NIOS adds the ability to view new cloud objects such as Tenants and VM IP addresses. You can view cloud objects and their related information in the Cloud tab of Grid Manager. The Cloud tab provides the following sub tabs for viewing different information related to cloud objects: Tenants, VPCs, Networks, VMs (by IP Address), and Cloud Platform Members.

In addition to viewing data in these tabs, you can do the following:

- Click the Action icon and select an action from the menu.
  - Select Show Active Users to view all the users who are currently active on the Active Directory domain. For information, see Viewing Active Users.
  - Modify some of the data in the table. Double click a row, and either modify the data in the field or select an item from a drop-down list.
  - Click Save to save the changes. Note that some fields are read-only.
  - Edit the properties of an object.
  - Select the object, and then click the Edit icon.
  - Export the list of objects to a .csv file.
    - Click the Export icon.
  - Print the list of objects.
    - Click the Print icon.
  - Use filters and the Goto function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Goto field and select the object from the possible matches.
  - Create a quick filter to save frequently used filter criteria:
    - In the filter section, click Show Filter and define filter criteria for the quick filter.
    - Click Save and complete the configuration in the SaveQuickFilter dialog box.

The appliance adds the quick filter to the quick filter drop-down list in the panel. Note that global filters are prefixed with [G], local filters with [L], and system filters with [S].

Viewing All Tenants

The Tenants tab lists all tenants from the CMP. Tenant is an abstract administrative concept. Similar to a tenant in the CMP, a tenant object in NIOS encompasses all network elements such as networks, zones, VMs, and IP addresses (fixed and floating), network views, default DNS view, and all related extensible attributes associated with that tenant. Multiple tenants can be mapped to the same network view. A tenant can also have VMs (with IP addresses) in its shared or external networks that are in different network views.

In Grid Manager, you can click a tenant name in the Cloud tab -> Tenants tab and drill down to the Networks and VMs (by IP Address) sub tabs to view networks and VMs associated with the selected tenant. In the Tenants tab -> VMs tab, you can click a VM name and drill down more to view the Networks and IP Addresses sub tabs for the selected VM. You can always click the bread crumb at the top of the viewer to go back to the Tenants home tab.

Each tenant has a name and a unique tenant ID. The tenant ID is provided through cloud API requests. You cannot create or delete tenant objects through Grid Manager. All tenants are created and deleted through cloud API requests. However, you can modify the name, extensible attributes, and permissions for a specified tenant through the Tenant editor in Grid Manager if you have valid tenant permissions: All Tenants or per tenant object. Note that you cannot delegate the authority of any given tenants.

To view all tenant objects:

1. From the Cloud tab, click the Tenants tab.
2. Grid Manager displays the following information for each tenant:

   - **Actions**: Click the action icon (shown as a gear in each row) next to a selected tenant and choose from the following:
     - **Edit**: Modify certain general properties.
     - **Extensible Attributes**: Add or modify extensible attributes.
     - **Permissions**: Modify the administrative permissions.
     - **Mgmt Platform**: Displays the CMP that manages this tenant. When it displays Amazon, it indicates a successful validation of the Amazon account from NIOS to AWS.
     - **Name**: The tenant name.
     - **ID**: The unique tenant ID.
- **VMs**: The total number of VM objects associated with this tenant. This can include the following object types: Host Record, Fixed Address, and any resource record type such as A, AAAA, PTR, and CNAME records. It also includes unmanaged IP addresses that are associated with the tenant.

- **Networks**: The total number of IPv4 and IPv6 networks and network containers associated with this tenant. Note that this number includes only networks and network containers created by the cloud adapter.

- **Created**: The timestamp when the tenant was first created. You cannot modify this field. This timestamp reflects the time when the tenant object was first seen by the Grid Master, so it may not match the timestamp when the original cloud API request was sent.

- **Last Updated**: The timestamp when the last event associated with this tenant happened. You cannot modify this field. This timestamp reflects the time when the last event associated with this tenant was processed by the Cloud Platform Appliance, so it may not match the timestamp when the original cloud API request was sent.

- **Comment**: Information about this tenant.

- **Network Views**: The network view to which this tenant belongs.

- **Managed**: Indicated whether this tenant is a managed or an unmanaged object in NIOS.

- **Site**: The value entered for this predefined extensible attribute.

You can also select other cloud extensible attributes for display by clicking the down arrow next to any column header and selecting **Columns -> Edit Columns**.

---

**Note**: The vDiscovery for the OpenStack management platform discovers all tenants if the OpenStack user has the admin role in at least one tenant.

---

**Viewing All VPCs (Virtual Private Clouds)**

The **VPCs** tab displays all AWS VPCs. You can also manage selected VPCs, primarily for changing permissions, defining or changing extensible attributes, and changing the delegation settings for a VPC to a different NIOS Cloud member. An Amazon VPC is analogous to a network container in NIOS, and is hence represented as a network container with a special icon.

To view all VPCs:

1. From the **Cloud** tab, click the **VPCs** tab.
2. Grid Manager displays the following information for each VPC:
   - **Actions**: Click the action icon (shown as a gear in each row) next to a selected tenant and choose from the following:
     - **Edit**: Modify certain general properties.
     - **Extensible Attributes**: Add or modify extensible attributes.
     - **Permissions**: Modify the administrative permissions.
   - **Mgmt Platform**: Displays the CMP that manages the VPC. When it displays *Amazon*, it indicates a successful validation of the Amazon account from NIOS to AWS.
   - **VPC Name**: The AWS virtual private cloud name. The name is automatically defined by AWS. Each VPC name is a link that opens the Networks tab for the selected VPC. This page lists the individual private networks that exist within the VPC.
   - **Networks**: The number of individual private networks contained in the VPC.
   - **VMs**: The number of Amazon EC2 virtual machine instances currently discovered in the VPC. (You can run a vDiscovery in any VPC.) For information about how to start a vDiscovery, see Configuring vDiscovery Jobs.
   - **Tenants**: The number of cloud tenants associated with each VPC.
   - **Cloud Usage**: Indicates whether the VPC is associated with any specific cloud extensible attributes or within a scope of delegation. It can be one of the following:
     - **Cloud from adapter**: Indicates that this object has been created by a cloud adapter and it may or may not be within a scope of delegation at the moment.
     - **Cloud from delegation**: Indicates that this object is within the scope of delegation or the object itself defines a scope of authority delegation, and it is not created by a cloud adapter.
     - **Used by cloud**: Indicates that this network or network container is associated with the extensible attribute Is External or Is Shared and the value is set to True, which implies the network is a private or shared network managed by the CMP, and it is not Cloud from adapter or Cloud from delegation.
     - **Non-cloud**: The object is a regular NIOS object and is not within the scope of any authority delegation nor is it associated with any of these extensible attributes: Cloud API Owned, Is External or Is Shared. NIOS admin users can modify this object based on their permissions.
   - **Owned By**: A cloud object can be owned by the Grid Master or the cloud adapter. When the object is created by the Grid Master, this shows Grid. If the object is created by the cloud adapter, this shows Cloud Adapter.
   - **Delegated to**: The NIOS Cloud appliance to which management of the AWS VPC is delegated. This field tells you whether or not a cloud object (in this case, a virtual private cloud) has been delegated to a Cloud Platform Appliance.
   - **Network**: The network IP. The network listed in this column for the VPC is also viewable from the main Data Management -> IP AM tab.
   - **Site**: Extensible Attribute listing the site information for the VPC.
   - **Availability Zone**: The Amazon availability zone in which the VPC resides.

You can also select other cloud extensible attributes for display by clicking the down arrow next to any column header and selecting **Columns -> Edit Columns**.
Viewing All Cloud Networks

The Networks tab displays all IPv4 and IPv6 networks and network containers from the CMP as well as all delegated networks. You can select a specific network or network container and modify its properties in the Cloud IPv4 Network or Cloud IPv6 Network editor.

To view all cloud networks and network containers:

1. From the Cloud tab, click the Networks tab.
2. Grid Manager displays the following information for each network and network container:
   - **Actions:** Click the action icon (shown as a gear in each row) next to a selected tenant and choose from the following:
     - **Go to Tenant:** Go to the Tenant tab to view associated tenant.
     - **Go to DHCP Network Details:** Go to the DHCP -> Networks tab to view associated details.
     - **Go To IPAM Network Details:** Go to the IPAM -> Networks tab to view associated details.
     - **Go To Network View Details:** Go to the IPAM -> Network View tab to view associated details.
     - **Edit:** Modify certain general properties.
     - **Extensible Attributes:** Add or modify extensible attributes.
     - **Permissions:** Modify the administrative permissions.
   - **Mgmt Platform:** Displays the cloud that manages the network. When it displays Amazon, it indicates a successful validation of the Amazon account from NIOS to AWS.
   - **Network:** The IP address and netmask of the network.
   - **Tenant:** The associated tenant for the network.
   - **VPC Name:** The name of the associated VPC in AWS.
   - **Cloud Usage:** This field indicates whether this object is associated with any specific cloud extensible attributes or within a scope of delegation. It can be one of the following:
     - **Cloud from adapter:** Indicates that this object has been created by a cloud adapter and it may or may not be within a scope of delegation at the moment.
     - **Cloud from delegation:** Indicates that this object is within the scope of delegation or the object itself defines a scope of authority delegation, and it is not created by a cloud adapter.
     - **Used by cloud:** Indicates that this network or network container is associated with the extensible attribute Is External or Is Shared and the value is set to True, which implies the network is a private or shared network managed by the CMP, and it is not Cloud from adapter or Cloud from delegation.
     - **Non-cloud:** The object is a regular NIOS object and is not within the scope of any authority delegation nor is it associated with any of these extensible attributes: Cloud API Owned, Is External or Is Shared. NIOS admin users can modify this object based on their permissions.
   - ** Owned By:** A cloud object can be owned by the Grid Master or the cloud adapter. When the object is created by the Grid Master, this shows Grid. If the object is created by the cloud adapter, this shows Adapter.
   - **Delegated To:** This tells you whether a cloud object has been delegated to a Cloud Platform Appliance or not. If the cloud object has a parent object and the parent has been delegated, this field shows the parent delegation and you cannot modify the field.

You can also select other cloud extensible attributes for display by clicking the down arrow next to any column header and selecting Columns -> Edit Columns.

Viewing All Cloud VMs

The VMs tab lists all cloud VMs by IP addresses. A VM object is an abstract object representing a virtual machine that is running on the CMP. A VM belongs to one and only one tenant. However, the same VM may have more than one IP addresses (including unmanaged IP addresses) associated with it. Each VM may have an IP address that is part of an overlapping private IP address space and one or more IP addresses in the shared or external networks.

A VM object in NIOS can be a collection of supported object types that have the same value for the extensible attribute VM ID. Only the following NIOS object types are considered as existing VMs when they are tagged with the VM ID attribute: Host Record, A Record, AAAA Record, and PTR Record, and Fixed Address. A VM object may be defined by objects from different network views, and it can have more than one IP addresses associated with it.

**Note:** Since a VM can be defined by objects from different network views, the same IP address may appear multiple times if it has been defined in more than one network view. A VM object is a read-only abstract object, therefore you cannot create, modify, or delete it.

After a vDiscovery job is completed, the appliance displays discovered data for each VM in this tab. Available data is displayed based on the vDiscovery configuration and your CMP. For example, if your CMP is AWS, discovered data can include the VPC to which the VM belongs. You can click a VM name and drill down to the Networks and IP Addresses sub tabs to view networks and IP addresses associated with the selected VM. For more information about vDiscovery, see Configuring vDiscovery Jobs.

Note that in addition to managing discovered data through Grid Manager, you can clear any managed or unmanaged discovered data, or clear all discovery data related to a vDiscovery job through a cloud API request. You can use this feature to properly identify VMs that you spin up or de-provision through a cloud adapter. For example, when you use Infoblox IPAM Plug-In for VMware as the cloud adapter to de-provision a VM, you can send a cloud API call to remove the discovered data for this VM so you can avoid IP address conflict with IP addresses manually.
allocated by the VMware vCenter. For information about cloud API requests, see About Cloud API Requests.

In the VMs tab, discovered VMs are highlighted in different background colors, as follows:

- **Yellow**: Unmanaged VMs that do not have associated NIOS objects.
- **White**: Discovered VMs that have at least one associated NIOS object and there is no conflicting information between the discovered data and the NIOS data.
- **Red**: Discovered VMs that have at least one associated NIOS object and there is conflicting information between the discovered data and the NIOS data. Depending on the nature of the conflict, you can resolve them as described in Resolving Conflicting Addresses. You may also be able to convert or clear unmanaged data, as described in Managing Unmanaged Data.

To view all VM objects in NIOS:

1. From the Cloud tab, click the VMs tab.
2. Grid Manager displays the following information for all cloud VM by IP address:
   - **Actions**: Click the action icon (shown as a gear in each row) next to a selected tenant and select the action you want to perform.
   - **Mgmt Platform**: Displays the CMP to which this tenant belongs. This can be Amazon, OpenStack, or VMware.
   - **VM Name**: The name of the VM.
   - **VM ID**: The unique tenant ID to which this VM belongs.
   - **Networks**: The number of networks that belong to this VM.
   - **IP Address**: The IP address of the VM.
   - **VM VPC**: The VPC to which this VM belongs.
   - **VM Tenant**: The tenant to which this VM belongs.
   - **Port ID**: The port ID for the VM.
   - **Network View**: The network view to which this VM belongs.
   - **Active Users**: The number of active users on the selected network.
   - **FQDN**: The FQDN of the VM.
   - **VM Last Updated**: The timestamp when the VM data was last updated.
   - **First Discovered**: The timestamp when the VM was first discovered.
   - **Last Discovered**: The timestamp when the VM was last discovered.
   - **Task Name**: The name of the task that collected the discovered data. It is usually the ID or task name that collected the discovered data.
   - **Comment**: Information about the VM.

Depending on your CMP, you can also select additional discovered fields to be displayed in the VMs tab by clicking the down arrow next to any column header and selecting Columns -> Edit Columns. Note that some of these fields contain discovered data that is only relevant to your CMP.

### Viewing All Cloud Platform Members

The Members tab displays all members that are currently running the cloud API service. To view all cloud members in NIOS:

1. From the Cloud tab, click the Members tab.
2. Grid Manager displays the following information for each member:
   - **Actions**: Click the action icon (shown as a gear in each row) next to a selected tenant and select the action you want to perform.
   - **Name**: The member name.
   - **Status**: The current status of this member.
   - **Comment**: Information about this cloud member.
   - **Site**: The value entered for this predefined extensible attribute.

Select other cloud extensible attributes for display by clicking the down arrow next to any column header and selecting Columns -> Edit Columns.

### Chapter 8 Managing Appliance Operations

Managing the operations of a NIOS appliance involves defining system parameters such as time, security, and port settings. It also includes configuring operations such as scheduling tasks, defining approval workflows, managing licenses, managing extensible attributes, and configuring access control for supported operations.

The tasks covered in this chapter include:

- 5800278
- Administrative Permissions
- Operations that Support Access Control
- Defining Named ACLs
- Managing Named ACLs
- Applying Access Control to Operations
- Managing Time Settings
- Changing Time and Date Settings
• Changing Time Zone Settings
• Monitoring Time Services

• Using NTP for Time Settings
  • Authenticating NTP
  • NIOS Appliances as NTP Clients
  • Configuring the Grid to Use NTP
  • Configuring Grid Members to Use NTP
  • NIOS Appliances as NTP Servers
  • Configuring a NIOS Appliance as an NTP Server
  • Monitoring NTP

• About Extensible Attributes
  • Adding Extensible Attributes
  • Configuring Inheritable Extensible Attributes
  • Using Extensible Attributes
  • Viewing Extensible Attributes
  • Modifying Extensible Attributes
  • Deleting Extensible Attributes
  • Configuration Examples for Inheritable Extensible Attributes

• Managing Security Operations
  • Restricting Remote Console Access
  • Restricting GUI/API Access
  • Enabling HTTP Redirection
  • Modifying the Session Timeout Setting
  • Disabling the LCD Input Buttons
  • Configuring Security Features
  • Enabling and Disabling Remote Console and Infoblox Technical Support Access

• Configuring Proxy Servers
  • Configuring Members and Interfaces for Automatic Updates

• Configuring Ethernet Ports
  • Enabling GUI and API Access on the MGMT and LAN1/VIP Ports
  • About Virtual LANs
  • Implementing Quality of Service Using DSCP
  • Ethernet Port Usage
  • Modifying Ethernet Port Settings
  • Using the LAN2 Port
  • About Port Redundancy
  • Configuring the LAN2 Port
  • Enabling DHCP on LAN2
  • Enabling DNS on LAN2

• Using the MGMT Port
  • Appliance Management
  • Grid Communications
  • DNS Services

• About Lights Out Management
  • Enabling LOM
  • Adding LOM User Accounts
  • Configuring the IPMI Network Interface
  • Modifying LOM Settings
  • Viewing LOM Users
  • IPMI Commands and Examples

• Setting Static Routes
• Enabling DNS Resolution

• Managing Licenses
  • License Types
  • Managing Static Licenses
  • Managing Dynamic Licenses
  • Managing Grid-wide Licenses
  • Adding Permanent or Subscription Licenses
  • Adding Temporary Licenses
  • Viewing Licenses
  • Backing Up Licenses
  • Removing Licenses

• About IB-FLEX
  • Limitations of IB-FLEX
  • About IB-FLEX Instances and Platform Settings
  • Configuring DNS Cache Acceleration on IB-FLEX
  • Reports for IB-FLEX

• About Elastic Scaling
  • Using Elastic Scaling to Pre-provision and Launch vNIOS Members
  • Generating Tokens for Grid Members
  • Using CLI Commands to Join Grid Members
  • Using OpenStack cloud-init template to configure Grid Master and join Grid members
Configuring Access Control

To effectively manage your core network services, you can grant legitimate hosts access to specific tasks and operations using an access control list (ACL) or anonymous access control entries (ACEs). Depending on your admin permissions, you can configure a named ACL, and then apply it to multiple operations, such as file distribution and DNS zone transfers. For information about admin permissions, see About Administrative Permissions.

When you define a named ACL, you add access control types such as IPv4 and IPv6 addresses, IPv4 and IPv6 networks, nested named ACLs, and TSIG key based ACEs to a list, and then grant each entry in the list the Allow or Deny permission. For information about named ACLs and how to configure them, see Defining Named ACLs. Note that each operation supports specific access control types. You cannot apply a named ACL to an operation that does not support the access control types contained in the named ACL. For more information about which NIOS operations support access control and which access control types each operation supports, see Operations that Support Access Control.

When you add or modify a named ACL, or when you import named ACLs and ACEs to an existing named ACL through CSV import, the appliance does not automatically validate the ACEs in the list. For more information about how to import named ACLs and ACEs, refer to the Infoblox CSV Import Reference. To avoid conflicts and unexpected results, you must perform validations for all named ACLs before you use them for access control. When the appliance detects a conflict or an optimized issue about a specific ACE during the validation process, it displays detailed information in a CSV file. For more information about ACL validation, see Validating Named ACLs.

Administrative Permissions

You can configure a named ACL at the Grid level and override it at the member and object level. Superusers and limited-access users with Read/Write permission to All Named ACLs can create, modify, and delete named ACLs. Users with Read-only permission to All Named ACLs can apply a named ACL to a supported object if they have Read/Write permission to the respective object. Other users can only view named ACLs and their entries. For information about admin permissions, see About Administrative Permissions.

Operations that Support Access Control

On the appliance, only certain operations support access control. You can apply one named ACL or multiple anonymous ACEs to each operation. However, you cannot apply multiple named ACLs or use a combination of named ACLs and ACEs. Note that each operation supports different access control types. For example, DNS zone transfers support IPv4 and IPv6 addresses and networks as well as TSIG key based ACEs, while AAAA filtering supports only IPv4 addresses and networks.

When you apply a named ACL to an operation, the appliance validates to ensure that the named ACL contains ACEs that are supported by the operation. The appliance also validates any new ACEs that you add to an existing named ACL. If a named ACL contains access control types that an operation does not support, the appliance displays an error message and you cannot apply that named ACL to the operation. Thus when defining a named ACL for a specific operation or applying an existing named ACL, ensure that it contains access control types that the operation supports. Table 8.1 lists access control types for NIOS operations that support access control.

<table>
<thead>
<tr>
<th>Operation Type</th>
<th>IPv4 Addresses and Networks</th>
<th>IPv6 Addresses and Networks</th>
<th>TSIG Key Based ACEs</th>
<th>DNSzone 2.x TSIG Key</th>
<th>Any Address and Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI and API Access</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>NTP Service and NTP Queries</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>File Distribution Services</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Syslog Proxy Access Control</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 8.1 Operations that Support Access Control
<table>
<thead>
<tr>
<th>Feature</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Zone Transfers (excludes zone transfers for Microsoft servers)*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic DNS Updates</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DNS Queries</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Recursive Queries</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Blackhole Lists</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>AAAA Filtering</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic DNS Updates</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Match Clients for DNS Views</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Match Destinations for DNS Views</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DNS64 Clients</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>DNS64 Mapped</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DNS64 Exclude IPv6</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note:** Zone transfers for Microsoft servers do not support named ACLs. However, you can still use individual ACEs to configure access control. For more information about how to configure zone transfer settings for Microsoft servers, see **Setting Zone Properties**. In addition, the DNSone 2.x TSIG key supports only the “Allow” permission. You cannot change “Allow” to “Deny.”

Complete the following tasks to use a named ACL:

1. Define a named ACL, as described in **Defining Named ACLs**.
2. Validate the named ACL, as described in **Validating Named ACLs**.
3. Apply the named ACL to specific operations, as described in **Applying Access Control to Operations**.

### Defining Named ACLs

Depending on how you plan to use a named ACL and which access control types an operation supports, you can add one or all of the following when you define a named ACL: IPv4 and IPv6 addresses, IPv4 and IPv6 networks, TSIG key based ACEs, DNSone 2.x TSIG keys. You can also add an existing named ACL as a nested ACL to a new or existing named ACL.

When configuring a named ACL, ensure that you define it correctly for the intended operations using the supported access control types. For example, if you want to apply a named ACL to AAAA filtering, do not include IPv6 addresses or networks in the named ACL because AAAA filtering does not support IPv6 addresses and networks. For information about supported access control types, see **Table 8.1**.

To define a named ACL:

1. From the **Administration** tab, select the **Named ACLs** tab, and then click the **Add** icon.
2. In the **Add Named ACL** wizard, complete the following:
   - **Name**: Enter a name for the named ACL. You can enter up to 64 characters.
   - **Comment**: Enter additional information about the named ACL.
3. Click **Next**. Complete the following to add ACEs to the named ACL:
   - Click the **Add** icon and select one of the following access control types from the drop-down list. Depending on your selection, Grid Manager adds a row to the table directly or expands the panel before adding a row:
     - **IPv4 Address**: Select this to add an IPv4 address. Click the **Entry** field and enter the IPv4 address. The **Operation** column displays **Allow** by default. You can change it to **Deny** by clicking the field and selecting **Deny** from the drop-down list.
     - **IPv4 Network**: When you select this, enter the network address in the **Address** field, select the netmask using the slider, and then select **Allow** or **Deny** from the **Permission** drop-down list. Click **Add** and Grid Manager adds the entry to the table.
     - **IPv6 Address**: Select this to add an IPv6 address. Click the **Entry** field and enter the IPv6 address. The **Operation** column displays **Allow** by default. You can change it to **Deny** by clicking the field and selecting **Deny** from the drop-down list.
     - **IPv6 Network**: When you select this, enter the network address and its netmask in the **Address** field, and then select **Allow** or **Deny** from the **Permission** drop-down list. Click **Add** and Grid Manager adds the entry to the table.
     - **TSIGKey**: In the **AddTSIGKey** panel, complete the following, and then click **Add** to add the TSIG key to the list:
       - **Key name**: Enter a meaningful name for the key, such as a zone name or the name of the remote name server. This name must match the name of the same TSIG key on other name servers.
       - **Key Algorithm**: Select either HMAC-MD5 or HMAC-SHA256.
       - **Key Data**: To use an existing TSIG key, type or paste the key in the **Key Data** field. Alternatively, you can select the key algorithm, select the key length from the **Generate Key Data** drop down list, and then click **Generate**.
rate Key Data to create a new key.

- **DNSone 2.x TSIG Key**: Select this when the client is a NIOS appliance running DNS One 2.x code. The appliance automatically populates the value of the key in the **Entry** field. The **Operation** column displays **Allow** by default. You cannot change the default permission.
- **Any Address/Network**: Select this to allow or deny permission for any addresses and networks.
- **Named ACL**: When you select this, Grid Manager displays the **Named ACLs** Selector. Select the named ACLs you want to add to the new ACL. If you have only one existing named ACL, Grid Manager automatically adds the named ACL to the list. The selected named ACL becomes a nested ACL in the newly created named ACL.

**Note**: The **Order** field in the table displays the position of each entry based on the order it is placed in the list. You can modify this number to change the order of an ACE. You can also select the ACE check box and use the up and down arrows next to the table to place the entry in the desired position.

4. Click **Next** to enter extensible attributes for the named ACL. For information, see **About Extensible Attributes**.

5. Save the configuration.

### Managing Named ACLs

You can do the following after you have configured named ACLs for access control:

- Preview the list of ACEs in a named ACL, as described in **Previewing ACEs in Named ACLs**.
- Validate ACEs in a named ACL, as described in **Validating Named ACLs**.
- View a complete list of configured named ACLs, as described in **Viewing Named ACLs**.
- Modify information in a named ACL, as described in **Modifying Named ACLs**.
- Apply a named ACL to supported operations, as described in **Applying Access Control to Operations**.
- Delete a named ACL, as described in **Deleting Named ACLs**.
- Export and print the list of named ACLs.

### Previewing ACEs in Named ACLs

You can preview the list of ACEs in a named ACL when you add or modify it. When you click the Preview icon in the **Add Named ACL** wizard or **Named ACL** editor, the appliance lists all the entries in the named ACL, even if you have selected only one or a few entries in the wizard or editor.

To preview a named ACL:

1. From the **Administration** tab, select the **Named ACLs** tab -> **named_acl** check box, and then click the Preview icon.
2. In a separate browser window, Grid Manager displays the following information for each ACE in the named ACL:
   - **Entry**: Displays one of the following: IPv4 or IPv6 address, IPv4 or IPv6 network, or TSIG key. Note that if the named ACL contains nested ACLs, all entries in the nested ACLs are displayed in a flat view. Grid Manager does not display the name of the nested ACL.
   - **Type**: The access control type of the entry. This can be IPv4 **Address**, IPv6 **Address**, IPv4 **Network**, IPv6 **Network**, **TSIG Key**, or **DNSone 2.x TSIG Key**.
   - **Operation**: Displays the access permission for the entry. This can be **Allow** or **Deny**.

### Validating Named ACLs

When you add or modify a named ACL, the appliance does not automatically validate the ACEs in the list. In addition, when you import named ACLs or ACEs to a named ACL, no automatic validation is performed. To avoid unintended consequences, ensure that you validate your named ACLs before you save them or use them for access control.

**Note**: When you click the Validate icon in the **Add Named ACL** wizard or **Named ACL** editor, the appliance validates all the entries in the named ACL, even if you have selected only one or a few entries in the wizard or editor.

The following examples demonstrate the importance of validating named ACLs:

**Example 1**
You configure a named ACL "foo" that includes a Deny permission to 10.0.0.0/16. You then assign "foo" to DNS zone transfers. You later import an "Allow/10.0.0.0/24" entry to "foo" through CSV import. The appliance appends the entry to the end of "foo." When you perform an ACL validation on "foo" after a DNS service restart, the appliance displays a warning message indicating that the new "Allow/10.0.0.0/24" entry is now included in the previously configured "Deny/10.0.0.0/16" entry. Since DNS service works on a first-match access control basis, zone transfers will not be allowed for the 10.0.0.0/24 network, which is probably not your original intent. You can then modify the named ACL to correct this error. On the other hand, if you do not perform the ACL validation, the appliance is not notified about the new network entry in "foo." As a result, you are not notified about the denial of zone transfers to 10.0.0.0/24.

**Example 2**
You add a nested named ACL "bar" as the first entry to the named ACL "foo." You then add a "Deny All" entry right after "bar" (as the second entry). You later import a new "Allow All" entry to "bar" through CSV import. The "Allow All" entry will be appended to the end of "bar." When you perform an ACL validation on "foo" after the CSV import, the appliance detects a conflict between the "Allow All" (in "bar") and "Deny All" (right after "bar") permissions and displays a warning. Imagine if you do not perform the ACL validation on "foo," the appliance is not notified about the new "Allow All" entry in "bar" and therefore cannot detect the conflict between the "Allow All" and "Deny All" entries. As a result, almost all hosts will get zone transfers, which may not be the outcome you have intended.
**Note:** It is important that you manually validate each named ACL after a CSV import to ensure data and performance integrity. The appliance does not automatically perform ACL validation.

**To validate a named ACL:**

1. From the Administration tab, select the Named ACLs tab -> named_acl check box, and then click the Validate icon.  
   or  
   In the Add Named ACL wizard or Named ACL editor, click the Validate icon.
2. Grid Manager validates all the ACEs in the named ACL and displays a system message at the top of the screen indicating whether all ACEs in the named ACL are valid or not, depending on the validation results. When the appliance detects conflicts or issues related to specific ACEs, it displays the results in a CSV file. You can save the file or open it. Grid Manager displays the following information in the file:
   - **Defined ACL:** The name of the named ACL.
   - **Type of Issue:** The type of issue found. This can be one of the following:
     - **Optimize:** An ACE is a duplicate of a previous entry or an ACE configuration can be a subset of another entry. See optimized suggestions in the Issue field.
     - **Conflict:** The same IP address or network has a conflicting permission. Re-configure the ACE based on your requirements.
     - **Warning:** An ACE is a subset of a previously configured entry, but it has a conflicting permission.
   - **ACE A:** The ACE that has a conflict or an optimized issue with ACE B.
   - **ACE B:** The ACE that has a conflict or an optimized issue with ACE A.
   - **Issue:** Detailed information and optimized suggestions about the conflict or issue.

**Note:** It may take a long time to validate a named ACL that contains a large number of ACEs.

**Viewing Named ACLs**

To view a list of named ACLs:

- From the Administration tab, select the Named ACLs tab. Grid Manager displays the following information for each named ACL:
  - **Name:** The name of the named ACL.
  - **Comment:** Information about the named ACL.
  - **Site:** The site to which the named ACL belongs. This is one of the predefined extensible attributes.

You can also do the following in the Named ACLs tab:

- Modify data in the table. Double click a row, and either modify the data in the field or select an item from a drop-down list. Click **Save** to save the changes or **Cancel** to exit.
- Sort the named ACLs in ascending or descending order by column.
- Select a named ACL and click the Edit icon to modify data, or click the Delete icon to delete it.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Print and export data in this tab.

**Modifying Named ACLs**

You can modify ACEs in an existing named ACL. When you update a named ACL, the appliance validates the updates to ensure that ACEs in the named ACL are valid for the operations to which the named ACL has been applied. For example, if a named ACL is used for file distribution access, you are not allowed to add IPv6 address access control to it because the file transfer operation does not support IPv6 addresses.

To modify a named ACL:

1. From the Administration tab, select the Named ACLs tab -> named_acl check box, and then click the Edit icon.
2. The Named ACL editor provides the following tabs from which you can modify data:
   - **Genera Basic:** You can modify data in this tab as described in Defining Named ACLs.
   - **Extensible Attributes:** Add and delete extensible attributes that are associated with a specific named ACL. You can also modify the values of the extensible attributes. For information, see About Extensible Attributes.
   - **Permissions:** This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions.

**Deleting Named ACLs**

When you delete a named ACL, the appliance puts it in the Recycle Bin, if enabled. You can restore the named ACL later if needed.

**Note:** You cannot delete a named ACL that has been applied to an operation or is currently in use by another operation.
To delete a named ACL:

1. From the Administration tab, select the Named ACLs tab -> named_acl check box, and then click the Delete icon. You can select multiple named ACLs for deletion.
2. In the Delete Confirmation dialog box, click Yes.

Applying Access Control to Operations

When you apply access control to NIOS operations, you can use anonymous ACEs or a named ACL. You cannot combine ACEs and named ACLs for access control. Depending on the access control types each operation supports, you may or may not be able to apply a named ACL to a specific operation. For information about which access control types each operation supports, see Table 8.1.

Note: If you disable access control or select None or Any for an operation, the appliance removes the previously applied named ACL or the configured anonymous ACEs. To avoid losing your ACE configuration, Infoblox recommends that you convert the ACEs to a named ACL.

For information about how to apply access control to each supported operation, see the following:

- DNS zone transfers, as described in Enabling Zone Transfers
- DNS queries, as described in Controlling DNS Queries
- Recursive queries, as described in Enabling Recursive Queries
- Dynamic DNS updates, as described in Enabling DNS Servers to Accept DDNS Updates
- AAAA filtering, as described in Controlling AAAA Records for IPv4 Clients
- Blackhole list, as described in Configuring a DNS Blackhole List
- Match clients list for DNS views, as described in Defining Match Clients Lists
- Match destinations for DNS views, as described in Defining a Match Destinations List
- DNS64 clients, DNS64 mapped IPv4 addresses, and DNS64 excluded IPv6 addresses, as described in SettingDNS64 Group Properties
- File distribution services, as described in Configuring Access Control for File Distribution
- Grid Manager and API access, as described in Configuring Security Features
- NTP access control, as described in Defining NTP Access Control
- Syslog proxy access, as described in Configuring Syslog for Grid Members

Managing Time Settings

You can define the date and time settings for your NIOS appliance using the Infoblox Appliance Startup Wizard. Alternatively, you can set the date and time of the appliance anytime after you first configure it if you did not do so using the startup wizard or if you need to change it if, for example, you move an appliance from a location in one time zone to a location in a different time zone. To set the date and time of the appliance, you can either manually enter the values or configure the appliance to synchronize its time with a public NTP server.

Changing Time and Date Settings

If you do not use the NTP service, you can set the date and time for a Grid.

Note: You cannot manually set the date and time if the NTP service is enabled.

To set the time and date for a Grid using the Grid Properties editor:

1. From the Grid tab, select the Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit.
2. In the General tab of the Grid Properties editor, complete the following:
   - Date: Click the calendar icon to select a date or enter the date in YYYY-MM-DD format.
   - Time: Click the clock icon to select a time or enter the time in HH:MM:SS format. For afternoon and evening hours, use the integers 13-24.
3. Save the configuration and click Restart if it appears at the top of the screen.

Note: Changing the date and time resets the application and terminates the management session.

Changing Time Zone Settings

Whether you enable NTP (Network Time Protocol) or manually configure the date and time, you must always set the time zone manually. You can set the time zone for a Grid, which then applies to all members. If different members are in different time zones, you can choose the time zone that applies to most members at the Grid level, and then override the setting for the remaining members.

Note: Changing the time zone does not reset the application nor does it terminate the management session.

To set the time zone for a Grid or member:

1. Grid: From the Grid tab, select the Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit.
2. Member: From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.
To override an inherited property, click Override next to it and complete the appropriate fields.

1. In the General tab of the editor, select the appropriate time zone.
2. Save the configuration and click Restart if it appears at the top of the screen.

Monitoring Time Services

In a Grid, the Grid Master and its members use an internal NTP daemon to synchronize their time. It is not user-configurable and functions regardless of how you set the time on the Grid Master. The Detailed Status panel contains an NTP Synchronization icon so you can monitor the internal NTP daemon that runs within a Grid to ensure the time among its members is synchronized.

To display the Detailed Status panel, from the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Detailed Status icon in the table toolbar of the Members panel. The following are descriptions of the NTP status icons in the Detailed Status panel:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td></td>
<td>The NTP service is running properly.</td>
</tr>
<tr>
<td>Yellow</td>
<td></td>
<td>The appliance is synchronizing its time.</td>
</tr>
<tr>
<td>Red</td>
<td></td>
<td>The NTP service is not running properly.</td>
</tr>
</tbody>
</table>

The out-of-sync state is usually resolved when all NTP clients catch up with the server.

Using NTP for Time Settings

**Note:** vNIOS Grid members on Riverbed can be NTP clients only.

NTP (Network Time Protocol) is a standard protocol that system clocks use to ensure their time is always accurate. Appliances that use NTP try to get their time as close as possible to UTC (Coordinated Universal Time), the standard timescale used worldwide. NTP uses UDP (User Datagram Protocol) on port 123 for communications between clients and servers.

NTP is based on a hierarchy where reference clocks are at the top. Reference clocks use different methods such as special receivers or satellite systems to synchronize their time to UTC. NTP servers on the first level of the hierarchy synchronize their time with the reference clocks, and serve time to clients as well. Each level in the hierarchy is a stratum; stratum-0 is a reference clock. Stratum-1 servers synchronize their clocks with reference clocks. Stratum-2 servers synchronize their clocks with stratum-1 servers, and so forth. The stratum number indicates the number of levels between the NTP server and the reference clock. A higher stratum number could indicate more variance between the NTP server and the reference clock.

You can configure a NIOS appliance to function as an NTP client that synchronizes its clock with an NTP server. For more information, see NIOS Appliances as NTP Clients. NTP clients typically use time information from at least three different sources to ensure reliability and a high degree of accuracy. There are a number of public NTP servers on the Internet with which the NIOS appliance can synchronize its clock. For a list of these servers, you can access [http://www.ntp.org](http://www.ntp.org). When NTP is configured, it listens on all interfaces, including the loopback interface on the NIOS appliance.

In a Grid, the Grid Master and Grid members can function as NTP clients that synchronize their clocks with external NTP servers. They can in turn function as NTP servers to other appliances in the network. For more information, see NIOS Appliances as NTP Servers. Note that when the Grid Master functions as an NTP server, it synchronizes its local clock with its NTP clients and does not synchronize time with any other external NTP server. This allows you to deploy multiple NTP servers to ensure accurate and reliable time across the network. To configure the Grid Master and Grid members as NTP clients, you must first enable the NTP service and configure external NTP servers at the Grid level. You can then configure the Grid Master and Grid members to override the Grid-level NTP servers and use their own external NTP servers. Note that a Grid member will not function as an NTP client if you do not enable the NTP service at the Grid level. A Grid member synchronizes its clock with the Grid Master if you do not configure it to use external NTP servers.

In case of leap second insertion, the Infoblox Grid handles the leap second over a period of time instead of performing a one-time adjustment. In other words, when using the Grid as the NTP server, it follows the standard NTP recovery process by slewing over a certain period of time when handling the leap second. The slewing process could therefore cause synchronization issues among NTP clients. The out-of-sync state is usually resolved when all NTP clients catch up with the server.

**Figure 8.1** illustrates how NIOS appliances (the Grid Master and Grid members) in a Grid function as the NTP server or the NTP client, depending on your NTP configuration.

**Note:** The NTP service supports both IPv4 and IPv6 networks.
Authenticating NTP

To prevent intruders from interfering with the time services on your network, you can authenticate communications between a NIOS appliance and a public NTP server, and between a NIOS appliance and external NTP clients. NTP communications within the Grid go through an encrypted VPN tunnel, so you do not have to enable authentication between members in a Grid.

NTP uses symmetric key cryptography, where the server and the client use the same algorithm and key to calculate and verify a MAC (message authentication code). The MAC is a digital thumbprint of the message that the receiver uses to verify the authenticity of a message. As shown in Figure 8.2, the NTP client administrator must first obtain the secret key information from the administrator of the NTP server. The server and the client must have the same key ID and data. Therefore, when you configure the NIOS appliance as an NTP client and want to use authentication, you must obtain the key information from the administrator of the external NTP server and enter the information on the NIOS appliance. When you configure a NIOS appliance as an NTP server, you must create a key and send the key information to clients in a secure manner. A key consists of the following:

- **Key Number**: A positive integer that identifies the key.
- **Key Type**: Specifies the key format and the algorithm used to calculate the MAC (message authentication code) of a message.
  - M: The key is a 1-31 character ASCII string using MD5 (Message Digest).
  - S: The key is a 64-bit hexadecimal number in DES (Data Encryption Standard) format. The high order 7 bits of each octet form the 56-bit key, and the low order bit of each octet is given a value so that the octet maintains odd parity. You must specify leading zeros so the key is exactly 16 hexadecimal digits long and maintains odd parity.
  - A: The key is a DES key written as a 1-8 character ASCII string.
  - N: The key is a 64-bit hexadecimal number in NTP format. It is the same as the S format, but the bits in each octet have been rotated one bit right so the parity bit is in the high order bit of the octet. You must specify leading zeros and odd parity must be maintained.
- **Key String**: The key data used to calculate the MAC. The format depends on the Key Type you select.

When the NTP client initiates a request for time services to the NTP server, it creates the MAC by using the agreed upon algorithm to compress the message and then encrypts the compressed message (which is also called a message digest) with the secret key. The client appends the MAC to the message it sends to the NTP server. When the NTP server receives the message from the client, it performs the same procedure on the message — it compresses the message it received, encrypts it with the secret key and generates the MAC. It then compares the MAC it created with the MAC it received. If they match, the server continues to process and respond to the message. If the MACs do not match, the receiver drops the message.

Figure 8.2 NTP Client Administrator Obtaining Secret Key from NTP Server Administrator
You can configure an independent NIOS appliance, a Grid Master, or any Grid member in a Grid as an NTP client that synchronizes its system clock with an external NTP server.

**Note:** You can configure NIOS appliance as NTP client in either IPv4, IPv6, or dual mode (IPv4 and IPv6) network environment.

When you enable a NIOS appliance to function as an NTP client, you must specify at least one NTP server with which the appliance can synchronize its clock. Infoblox recommends that you specify multiple NTP servers that synchronize their time with different reference clocks and that have different network paths. This increases stability and reduces risk in case a server fails. For a list of public NTP servers, you can access www.ntp.org.

When you specify multiple NTP servers, the NTP daemon on the appliance determines the best source of time by calculating round-trip time, network delay, and other factors that affect the accuracy of the time. NTP periodically polls the servers and adjusts the time on the appliance until it matches the best source of time. If the difference between the appliance and the server is less than five minutes, the appliance adjusts the time gradually until the clock time matches the NTP server. If the difference in time is more than five minutes, the appliance immediately synchronizes its time to match that of the NTP server.

To secure communications between a NIOS appliance and an NTP server, you can authenticate communications between the appliance and the NTP server. When you configure authentication, you must obtain the key information from the administrator of the NTP server and enter the key on the appliance. For information, see Authenticating NTP.

In a Grid, you can configure the Grid Master and Grid members to synchronize their clocks with external NTP servers. When you enable the NTP service on the Grid, the Grid Master automatically functions as an NTP server to the Grid members. A Grid member can synchronize its time with the Grid Master, an external NTP server, or another Grid member. When Grid members synchronize their times with the Grid Master, the Grid Master and its members send NTP messages through an encrypted VPN tunnel, as shown in Figure 8.3. When a Grid member synchronizes its time with another Grid member, the NTP messages are not sent through a VPN tunnel.

*Figure 8.3 Grid Master as NTP Client*
1. Configuring the Grid to Use NTP

In a Grid, the Grid Master and Grid members can synchronize their clocks with external NTP servers. They then forward the clock time to other appliances in the network. Likewise, in an independent HA pair, the active node communicates directly with an external NTP server. The passive node then synchronizes its clock with the active node.

In a Grid, you must first enable the NTP service and configure external NTP servers at the Grid level before you configure the Grid Master and Grid members as NTP clients.

To configure a Grid Master as an NTP client, perform the following tasks:

- If you want to enable authentication between the Grid members and NTP servers, you must specify the authentication keys before enabling the NTP service. You can specify authentication keys at the Grid and member levels. For information, see Adding NTP Authentication Keys.
- Enable the NTP service on the Grid and specify one or more external NTP servers. For information, see Synchronizing the Grid with External NTP Servers.

Adding NTP Authentication Keys

To enable authentication between the appliance and the NTP servers, add the authentication keys before enabling the NTP service on the Grid. You can specify authentication keys at the Grid and member levels.

To add NTP authentication keys:

1. **Grid**: From the Grid tab, select the Grid Manager tab, expand the Toolbar and click NTP -> NTP Grid Config.
2. **Member**: From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box. Expand the Toolbar and click NTP Member Config.

To override an inherited property, click Override next to it and complete the appropriate fields.

3. Click the Add icon in the NTP Keys section and enter the following information.

   - **Key Number**: A positive integer that identifies a key.
   - **Type**: Specifies the key format and the algorithm used to calculate the MAC (message authentication code) of a message.
     - **MDS in ASCII format (M)**: The key is a 1-31 character ASCII string using MDS (Message Digest).
     - **DES in hex format (S)**: The key is a 64-bit hexadecimal number in DES (Data Encryption Standard) format. The high order 7 bits of each octet form the 56-bit key, and the low order bit of each octet is given a value so that the octet maintains odd parity. You must specify leading zeros so the key is exactly 16 hexadecimal digits long and maintains odd parity.
Synchronizing the Grid with External NTP Servers

To enable the Grid to synchronize its time with external NTP servers:

1. From the Grid tab, select the Grid Manager tab, expand the Toolbar and click NTP -> NTP Grid Config.
2. In the General tab of the Grid NTP Properties editor, select Synchronize the Grid with these External NTP Servers.
3. Click the Add icon to add external NTP servers and enter the following information in the Add NTP Server dialog box:
   - NTP Server (FQDN or IP Address): Enter either the IP address or the resolvable host name of an NTP server. Entries may be an IPv4 or IPv6 address. You can view a list of public NTP servers at ntp.isc.org. To check whether the DNS server can resolve the NTP server host name, click Resolve Name. You must have a DNS name resolver configured. For information, see Enabling DNS Resolution.
   - Enable Authentication: Select this option to enable authentication of NTP communications between the external NTP server and the NIOS appliance (the Grid Master or Grid member in a Grid, an independent NIOS appliance, or the active node in an independent HA pair).

   **Note:** To prevent intruders from interfering with the time services on your network, you can authenticate communications between a Grid member and an external NTP server, as well as between a Grid member and external NTP clients. NTP communications within the Grid go through an encrypted VPN tunnel, so you do not have to enable authentication between the Grid Master and Grid members.

   **Authentication Key:** Select a key that you previously entered from the drop-down list.
   - Click Add to add the NTP server to the list or Cancel to cancel the operation. In the table, you can configure some of the following settings:
     - Preferred: Select this to mark an external NTP server as the preferred NTP server. You can select only one server as the preferred NTP server. NIOS uses the responses from this preferred server over responses from other external NTP servers. A response from a preferred server will be discarded if it differs significantly from the responses of other servers. Infoblox recommends that you select an NTP server that is known to be highly accurate as the preferred server, such as one that has special time monitoring hardware. Note that this option is enabled only when you have selected the check box Synchronize the Grid with these External NTP Servers.
     - Server: Displays the FQDN or IP address of the NTP server that you added.
     - Authentication: When you enable authentication, this column displays Yes. Otherwise, it displays No.
     - Key Number: Displays the authentication key that you have selected.
     - BURST: Select this check box to configure the NTP client to send a burst of eight packets if the external NTP server is reachable and a valid source of synchronization is available. The NTP client transmits each packet at a regular interval of two seconds. After you add an NTP server and save the configuration, the appliance will enable this option by default. When you deselect this check box, the client sends a single packet only once to the server.
     - IBURST: Select this check box to configure the NTP client to send a burst of eight packets if the external NTP server is not reachable when the client sends the first packet to the server. The NTP client transmits each packet at a regular interval of two seconds. After you add an NTP server and save the configuration, the appliance will enable this option by default. When you deselect this check box, the client sends a single packet only once to the server.

   For information about adding NTP authentication keys, see Adding NTP Authentication Keys.
4. Save the configuration and click Restart if it appears at the top of the screen.

Configuring Grid Members to Use NTP

Once you configure a Grid member to use external NTP server, make sure that the NTP service is enabled at Grid level. Otherwise, the Grid member will not function as an NTP client. For information, see Synchronizing the Grid with External NTP Servers.

To configure Grid members to synchronize their time with external NTP servers:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box.
2. Expand the Toolbar and click NTP -> NTP Member Config.
3. In the General tab of the Member NTP Properties editor, do the following:
   - Enable the NTP Server on this Member: Select this check box to configure a Grid Master or a Grid member as an NTP server. If you have configured DNS anycast on the appliance, it can answer NTP requests through the anycast IP address.
   - Synchronize this Member only with the Grid Master: Select this check box to enable this Grid member to synchronize its time with the Grid Master. This is the default.
   - Synchronize this Member with other NTP Servers: Select this check box to enable this Grid member to use external NTP
servers. When you select this check box, you must enter at least one external NTP server for the member.

- **Exclude the Grid Master as an NTP Server:** Select this check box if you want to exclude the Grid Master from being one of the time sources. By default, the appliance automatically configures the Grid Master as the backup NTP server for a Grid member. When the member cannot reach any of its configured NTP servers, it uses the Grid Master as the NTP server. The appliance does not display the Grid Master in the NTP external server list. For a Grid Master, this check box has no meaning.

- **External NTP Servers:** Click **Override** and then click the **Add** icon. In the **Add NTP Server** dialog box, enter the following information:
  - **NTP Server (FQDN or IP Address):** Enter either the IP address or the resolvable host name of an NTP server. You can view a list of public NTP servers at ntp.isc.org. To check whether the DNS server can resolve the NTP server host name, click **Resolve Name.** You must have a DNS name resolver configured.
  - **Enable Authentication:** Select this check box to enable authentication of NTP communications between the external NTP server and the NIOS appliance (the Grid Master or Grid member in a Grid, an independent NIOS appliance, or the active node in an independent HA pair).

  **Note:** To prevent intruders from interfering with the time services on your network, you can authenticate communications between a Grid member and an external NTP server, as well as between a Grid member and external NTP clients. NTP communications within the Grid go through an encrypted VPN tunnel, so you do not have to enable authentication between the Grid Master and Grid members.

  **Authentication Key:** Select a key that you previously entered from the drop-down list. Note that you must enter authentication keys at the Grid level when you configure a Grid Master or Grid member to use external NTP servers.

- **Click **Add** to add the NTP server to the list or **Cancel** to cancel the operation. In the table, click **Override** in the table to override configurable settings. To inherit the same properties as the Grid, click **Inherit.**
  - **Preferred:** Select this to mark an external NTP server as the preferred NTP server. You can select only one server as the preferred NTP server. NIOS uses the responses from this preferred server over responses from other external NTP servers. A response from a preferred server will be discarded if it differs significantly from the responses of other servers. Infoblox recommends that you select an NTP server that is known to be highly accurate as the preferred server, such as one that has special time monitoring hardware. Note that this option is enabled only when you have selected the check box **Synchronize this Member with other NTP Servers.**
  - **Server:** Displays the FQDN or IP address of the NTP server that you added.
  - **Authentication:** When you enable authentication, this column displays **Yes.** Otherwise, it displays **No.**
  - **Key Number:** Displays the authentication key that you have selected.
  - **BURST:** Select this check box to configure the NTP client to send a burst of eight packets if the external NTP server is reachable and a valid source of synchronization is available. The NTP client transmits each packet at a regular interval of two seconds. After you add an NTP server and save the configuration, the appliance will enable this option by default. When you deselect this check box, the client sends a single packet only once to the server.
  - **IBURST:** Select this check box to configure the NTP client to send a burst of eight packets if the external NTP server is not reachable when the client sends the first packet to the server. The NTP client transmits each packet at a regular interval of two seconds. After you add an NTP server and save the configuration, the appliance will enable this option by default. When you deselect this check box, the client sends a single packet only once to the server.

  **Note:** NTP members inherit NTP properties from the Grid. Click **Override** in the **Member NTP Properties** wizard to override configurable settings. To inherit the same properties as the Grid, click **Inherit.**

  For information about adding NTP authentication keys, see **Adding NTP Authentication Keys.**

4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Managing External NTP Servers

You can specify multiple NTP servers for failover purposes. The NIOS appliance attempts to connect to the NTP servers in the order they are listed. A Grid member uses the Grid Master as the NTP server when it cannot reach any of its external NTP servers. You can change the order of the list by selecting an NTP server and dragging it to its new location or by clicking the up and down arrows. You can add and delete servers and modify their information as well.

### NIOS Appliances as NTP Servers

After you enable NTP on a Grid, the Grid members—including the Grid Master—can function as NTP servers to clients in different segments of the network. Similarly, after you enable NTP on an independent appliance or an HA pair, and it synchronizes its time with an NTP server, you can configure it to function as an NTP server as well. When you configure DNS anycast addressing on a Grid member and use it as an NTP server, the member can answer NTP requests from other NTP clients through the anycast IP address.

*Figure 8.4 Grid Members as NTP Servers*
To configure a NIOS appliance as an NTP server, perform the following tasks:

- Enable the appliance as an NTP server.
- Enable authentication between the appliance and its NTP clients.
- Optionally, specify which clients can access the NTP service of the appliance.
- Optionally, specify which clients can use ntpq to query the appliance.

Configuring a NIOS Appliance as an NTP Server

You can configure a Grid member—including the Grid Master—or an independent appliance or HA pair to function as an NTP server. When you enable a NIOS appliance to function as an NTP server, you can enable authentication between a NIOS appliance functioning as an NTP server and its NTP clients. When you enable authentication, you must specify the keys that the appliance and its clients must use for authentication. In a Grid, you can enter NTP authentication keys at the Grid level so that all the members can use them to authenticate their clients. You can also enter keys at the member level, if you want that member to use different keys from those set at the Grid level. After you enter the keys, you can download the key file and distribute the file to the NTP clients.

On an HA member, the NTP service runs on the active node. If there is an HA failover, the NTP service is automatically launched after the passive node becomes active and the NTP traffic uses the HA port on one of the nodes from an HA pair, instead of the LAN1 port. You might receive an error message indicating that the NTP is out of synchronization. During another HA failover, the currently passive node becomes active again and the NTP traffic uses the LAN1 port, and the NTP is back in synchronization. For information, see About HA Pairs.

To enable an appliance as an NTP server and authenticate NTP traffic between a NIOS appliance and an NTP client, perform the following tasks:

- Enable an appliance as an NTP server and define authentication keys. For information, see Enabling an Appliance as an NTP Server.
- Optionally, define NTP access control, including KoD packet configuration. For information, see Defining NTP Access Control.
- Optionally, configure anycast addressing for DNS and use the anycast IP address for NTP requests. For information about how to configure DNS anycast, see Configuring Anycast Addresses.

Enabling an Appliance as an NTP Server
To enable an appliance as an NTP server and add authentication keys:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box.
2. Expand the Toolbar and click NTP -> NTP Member Config.
3. In the General tab of the Member NTP Properties editor, do the following:
   - Enable the NTP Server on this Member: Select this option to configure a Grid Master or a Grid member as an NTP server. If you have configured DNS anycast on the appliance, it can answer NTP requests through the anycast IP address.
   - Click Override in the NTP Keys section to enter NTP authentication keys at the member level. The member uses these keys when acting as an NTP server and authenticates requests from NTP clients. Clear the check box to use the Grid-level authentication keys.
4. Click Add in the NTP Keys section. For information, see Adding NTP Authentication Keys.
5. Save the configuration and click Restart if it appears at the top of the screen.

After you enter the authentication keys, you can download the key file (usually called ntp.keys) and distribute it to NTP clients as follows:

1. Grid: From the Grid tab, select the Grid Manager tab.
   - Member: From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box.
2. Expand the Toolbar and click NTP -> Download NTP Keys.
3. In the Opening ntp.keys dialog box, save the file, and then click OK.
4. Distribute this to the NTP clients using a secure transport.

Defining NTP Access Control

The NTP access control list specifies which clients can use a NIOS appliance as an NTP server. If you do not configure access control, then the NIOS appliance allows access to all clients. You can configure access control at the NTP Grid level and override that at the member level.

In addition, the NIOS appliance can accept queries from clients using ntpq, the standard utility program used to query NTP servers about their status and operational parameters. You can specify from which clients the NIOS appliance is allowed to accept ntpq queries. The appliance does not accept ntpq queries from any client, by default.

You can use an existing named ACL (access control list) or multiple ACEs (access control entries) to control which clients can use the NIOS appliance as an NTP server, as well as those clients from which the appliance can accept queries using ntpq. For information about access control, see Configuring Access Control.

To specify which clients can access the NTP service of a NIOS appliance and from which clients a NIOS appliance can accept ntpq queries, and to enable or disable KoD, complete the following:

1. Grid: From the Grid tab, select the Grid Manager tab.
   - Member: From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box.
2. In the General tab of the Grid or Member NTP Properties editor, select one of the following to configure NTP access control:
   - None: Select this if you do not want to configure access control for NTP service. When you select None, the appliance allows all clients to access the NTP service. This is selected by default.
   - Use Named ACL for Time only: Select this and click Select Named ACL to select a named ACL that contains only IPv4 addresses and networks. NTP queries do not support TSIG key based ACEs. When you select this, the appliance allows clients that have the Allow permission in the named ACL to use its NTP service. NTP queries from the named ACL entries specified here are denied. You can click Clear to remove the selected named ACL and the appliance accepts ntpq queries from those NTP clients.
   - Use Named ACL for Time + NTP Control (NTPQ): Select this and click Select Named ACL to select a named ACL that contains only IPv4 addresses and networks. NTP queries do not support TSIG key based ACEs. When you select this, the appliance allows clients that have the Allow permission in the named ACL to use its NTP service, and for the appliance to accept ntpq queries from those clients as well. You can click Clear to remove the selected named ACL.
   - Use this set of ACEs: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows:
     - IPv4 Address: Select this to add an IPv4 address. Click the Value field and enter the IPv4 address. The default permission is Allow, which means that the appliance allows access to and from this IPv4 client. You cannot change the default permission. In the Service field, select Time only to allow this client for using the NTP service on the appliance; or select Time + NTP Control (NTPQ) to also accept ntpq queries from this client.
     - IPv4 Network: Select this to add an IPv4 network. Click the Value field and enter the IPv4 network. The default permission is Allow, which means that the appliance allows access to and from this IPv4 network. You cannot change the default permission. In the Service field, select Time only to allow this network for using the NTP service on the appliance; or select Time + NTP Control (NTPQ) to also accept ntpq queries from this network.
     - IPv6 Address: Select this to add an IPv6 address. Click the Value field and enter the IPv6 address. The default permission is Allow, which means that the appliance allows access to and from this IPv6 client. You cannot change the default permission. In the Service field, select Time only to allow this client for using the NTP service on the appliance; or select Time + NTP Control (NTPQ) to also accept ntpq queries from this client.
     - IPv6 Network: Select this to add an IPv6 network. Click the Value field and enter the IPv6 network. The default permission is Allow, which means that the appliance allows access to and from this IPv6 network. You cannot change the default permission. In the Service field, select Time only to allow this network for using the NTP service on the appliance; or select Time + NTP Control (NTPQ) to also accept ntpq queries from this network.
     - Any Address/Network: Select this to allow access to all IPv4 and IPv6 addresses and networks. The default
permission is **Allow**, which means that the appliance allows access to and from all IPv4 and IPv6 clients. You cannot change the default permission. In the **Service** field, select **Time only** to allow clients for using the NTP service on the appliance; or select **Time + NTP Control (NTPQ)** to also accept `ntpq` queries from all clients. After you have added access control entries, you can do the following:

- Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL icon and enter a name in the Convert to Named ACL dialog box. The appliance creates a new named ACL and adds it to the Named ACL panel. Note that the ACEs you configure for this operation stay intact.
- Reorder the list of ACEs using the up and down arrows next to the table.
- Select an ACE and click the Edit icon to modify the entry.
- Select an ACE and click the Delete icon to delete the entry. You can select multiple ACEs for deletion.
- **Enable KoD:** When you select this check box, the appliance (when acting as an NTP server) sends a KoD (Kiss-o’-Death) packet to the NTP client if the client has exceeded the rate limit. The KoD packet contains the stratum field set to zero and the ASCII string in the Reference Source Identifier field set to RATE, indicating the packets sent by the client have been dropped by the server. When you clear the check box, the NTP server drops the packets but does not send any KoD packet to the client. This check box is deselected by default. For more information about KoD, see **Enabling Kiss-o’-Death for NTP**.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

### Enabling Kiss-o’-Death for NTP

When an NTP server denies service to an NTP client, which has exceeded the rate limit, it typically drops the packets without notifying the client. In this case, the client, unaware of the situation, continues to transmit packets. To notify the client so it either slows down or stops the packet transmission, you can enable the NIOS appliance (when acting as an NTP server) to transmit a KoD (Kiss-o’-Death) packet. This packet contains the stratum field set to zero, implying the sent packet was invalid, and the ASCII string that contains RATE in the reference identifier field, indicating the status of the transmitted packet and access control. When the client receives the KoD packet, it may reduce transmission rate or stop packet transmission to the server. For more information about KoD, refer to **RFC 5905** (*Network Time Protocol Version 4: Protocol and Algorithms Specification*). You can enable KoD at the Grid level and override it at the member level. For more information about enabling KoD, see **Defining NTP Access Control**.

### Monitoring NTP

When you enable the Grid to synchronize its time with external NTP servers, you can monitor the status of the NTP service by checking the NTP status icons in the **Member Services** panel. To access the panel, from the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **Grid members** check box, and then select the Manage Member Services icon in the table toolbar of the Members tab. The following are descriptions of the NTP status icons in the **Members Services** panel. The type of information that can appear in the **Description** column corresponds to the SNMP trap messages. For information about the Infoblox SNMP traps, see **Chapter 37, Monitoring the Appliance**.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>The NTP service is enabled and running properly.</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>The NTP service is enabled, and the appliance is synchronizing its time.</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>The NTP service is enabled, but it is not running properly or is out of synchronization.</td>
</tr>
<tr>
<td></td>
<td>Gray</td>
<td>The NTP service is disabled.</td>
</tr>
</tbody>
</table>

After you upgrade the Grid to 6.6.x or later, the color of the Grid status icon changes based on the following:

- If you activate an external synchronization, or start the NTP service using the Grid Manager, or do not configure any external NTP servers, except local, then the NTP behavior remains the same and the NIOS appliance displays the Grid status icon in green.
- If you activate an external synchronization and configure one or more external NTP servers, or if the servers are in synchronization with the Grid Master, then the Grid status icon is as follows:
  - Green: NTP is synchronizing with an external server.
  - Red: NTP is synchronizing with the local server and at least one external NTP server is reachable. This status icon also indicates if there are problems with the NTP service.
  - Yellow: NTP is synchronizing with the local server and at least one external NTP server is reachable; but there could be problems on the external server, such as an exceeded root distance error.

### About Extensible Attributes

Extensible attributes are identifiers that you use to further define and track a NIOS object. For example, to specify the location of a network, you can add the predefined attribute **Site** and enter a specific location for the network. You can also specify whether an extensible attribute is required for an object or restrict the values that can be entered when you create a new object. You can also specify if an extensible attribute is inheritable by other objects in an inheritance chain. When you enable the inheritance of an extensible attribute, all descendants in the inheritance chain can inherit the extensible attribute so you do not have to configure it at all object levels. For example, if you define an extensible attribute for a network, the attribute and its value can be automatically added for DHCP ranges and fixed addresses in the network.
An extensible attribute is inheritable by descendants in an inheritance chain if its definition does not restrict it to objects that are not part of an inheritance chain. The appliance supports this inheritance chain: Network View -> Network Container -> Network -> Range -> Host/Fixed Address/Reservation. A parent object can have descendants at one or more levels. For example, a network view, network container, network, or DHCP range can be a parent object and have descendants at one or more levels, while a host, fixed address, and reservation can only be a descendant, not a parent. You can set an extensible attribute to be inheritable by selecting the Enable Inheritance option when you define an attribute. For more information, see Configuring Inheritable Extensible Attributes.

Note: Only superusers can configure extensible attributes.

You can use predefined extensible attributes or specify new ones for different objects. The appliance provides the following predefined extensible attributes that you can customize:

- Region
- Country
- State
- Site
- Building
- VLAN
- ReportingSite (Report Clustering)

When you use a predefined attribute, you can modify it and change its name, but you cannot change the type of data it accepts. You can also delete predefined attributes that you do not use. All predefined attributes accept text strings. You can define other settings though, as described in Modifying Extensible Attributes. You can also create your own extensible attributes, as described in Adding Extensible Attributes.

For example, you can configure the predefined attribute Site for fixed addresses and hosts, and define a new attribute Department for admin groups.

When you configure an extensible attribute, you can specify the following:

- The type of data that admins enter, such as text strings, integers, or email addresses. You can also restrict admins to a list of values.
- Whether admins can enter multiple values
- A default value
- Whether the attribute is required
- Whether the attribute is inheritable
- The objects associated with the attribute, such as admin groups, DNS views, or DHCP networks.
- Whether the appliance makes an entry in the audit log each time an object with the attribute is added or modified.

Activities such as additions, modifications, and deletions of inheritable extensible attributes, are recorded in the audit log. For information about how to use the audit log, see Using the Audit Log.

Figure 8.5 illustrates a network with different device types. Each device is represented as a host in the NIOS appliance database. You can configure Device Type, Location and Owner as required attributes for hosts. Then when admins add hosts, they will be required to enter values for these attributes in the Extensible Attributes tab of the Add Host wizard.

Figure 8.5 Using Extensible Attributes to Define Network Devices
After you configure extensible attributes for an object, the attributes become available in the **Extensible Attributes** tab of the wizard and editor of the corresponding object. Users then add or edit the attribute values, based on your configuration. Users can also specify attributes when searching for data and add attributes as columns in the tables of Grid Manager. For example, you can add the predefined **Site** attribute as a column in the Records panel of the **Zones** tab. For information about adding columns to tables, see **Customizing Tables**.

Users can also group objects in smart folders according to their attributes. For example, a user can create a smart folder that contains all networks in a certain site.

Users can enable the appliance to group members by extensible attributes. For information, see **Grouping Members by Extensible Attributes**.

When you first enable Cloud Network Automation, NIOS installs a set of extensible attributes that are specific for cloud usage. For more information, see **Extensible Attributes for Cloud Objects**.

### Adding Extensible Attributes

To add a new extensible attribute:

1. From the **Administration** tab, select the **Extensible Attributes** tab.
2. Click the Add icon on any of the toolbars.
3. In the **Add Extensible Attribute** wizard, complete the following:
   - **Name**: Enter the name of the attribute. This is a required field and is case-sensitive. You can enter up to 128 UTF-8 characters.
   - **Type**: Specify the type of data that you want to capture for an object. Select one of the following:
     - **String**: Select this when the attribute is used to define string values, such as names. When you select this type, the wizard displays the **Number of Characters** field where you can enter the minimum and maximum number of characters that users can enter.
     - **List**: Select this when you want to define a list of values for the attribute. Users can then select a value from this list. For example, if you want to restrict an attribute to five specific values, you can define the attribute as a **List** and then list the five values in the **List Values** section. When a user uses the attribute, they are limited to selecting from one of the five values. When you select **List**, the wizard displays the List of values table, where you add the allowed values. These values appear in the drop-down list when a user defines the attribute. Click the Add icon to enter values in the table. You can enter up to 64 UTF-8 characters for each value.
     - **Email**: Select this when the attribute is used for email addresses. Email addresses are entered in the format `user@dom`.

   You can also modify list values at a later time. When you modify list values, all object attributes using the modified values are updated to the new values.
   You can also delete values from the list. Note that when you delete a list value, all attributes using the deleted values are removed from the objects. For objects with multiple attribute values, only the deleted values are removed.
   You can also move a value up or down in the list.
   - **Integer**: Select this when the attribute is used to track whole numbers, such as serial numbers. When you select this type, the wizard displays the **Value Limits** fields where you can enter the range of allowed values. Note that you cannot change your entries in the **Value Limits** fields if you modify the attribute at a later date.
   - **Number of Characters**: When you select **String**, the wizard displays the **Number of Characters** field where you can enter the minimum and maximum number of characters that users can enter.

   You can also modify list values at a later time. When you modify list values, all object attributes using the modified values are updated to the new values. You can also delete values from the list. Note that when you delete a list value, all attributes using the deleted values are removed from the objects. For objects with multiple attribute values, only the deleted values are removed.
   You can also move a value up or down in the list.

   You can also modify list values at a later time. When you modify list values, all object attributes using the modified values are updated to the new values. You can also delete values from the list. Note that when you delete a list value, all attributes using the deleted values are removed from the objects. For objects with multiple attribute values, only the deleted values are removed.
   You can also move a value up or down in the list.
Configuring Inheritable Extensible Attributes

An extensible attribute can be inherited by descendants when it is at the top or in the middle of the inheritance chain. When you add a new extensible attribute to a parent object, the same extensible attribute may or may not already exist at the descendant levels. If the extensible attribute exists on a descendant, you can choose to have the descendant inherit the value from the parent, or retain the original value from the descendant. When the extensible attribute does not exist on the descendant, you can choose to have the descendant either inherit the extensible attribute and its value from the parent or not inherit anything from the parent.

When you add a range, host, fixed address or IPv4 reservation to a parent object which has inheritable extensible attributes, the newly added object can inherit extensible attributes from the parent object. For example, if you create an IPv4 network with inheritable extensible attributes, and then add a host, the values you specified for the extensible attributes while creating the network can be inherited by the host.

To assist you in identifying whether an extensible attribute value is inherited or overridden, the appliance displays the inheritance state of an attribute in the Inheritance State column of an extensible attribute. This column is displayed only for objects that support inheritance. For information about how to view inheritance states, see Modifying Inheritable Extensible Attributes.

Following are the supported inheritance states:

**Note:** Infoblox recommends that you define values for mandatory extensible attributes using the Grid only and do not use PAPI or RESTful API to define values.
Table 8.2 Inheritance States

<table>
<thead>
<tr>
<th>Inheritance</th>
<th>State Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherited</td>
<td>The extensible attribute inherits its value from the parent. You cannot edit the value of an attribute when the inheritance state is set to Inherited. You can change the state to Overridden and then change the value of the attribute or change the state to Not Inherited to remove the inherited value.</td>
</tr>
<tr>
<td>Overridden</td>
<td>The extensible attribute overrides the value inherited from the parent. You can change the state to Inherited and restore the original inherited value or change the state to Not Inherited and remove the inherited value.</td>
</tr>
<tr>
<td>Not Inherited</td>
<td>The extensible attribute can inherit its value from the parent, but the attribute does not exist on the descendant. You can change the state to Inherited and restore the original inherited value or change the state to Overridden and change the value of the attribute. Note that when the state of an inheritable extensible attribute is Not Inherited, the corresponding attribute will not be added as a new extensible attribute for objects that are currently not inheriting this extensible attribute.</td>
</tr>
<tr>
<td>No Parent</td>
<td>The inheritance state is set to No Parent when an object has a parent, but the parent does not have an extensible attribute or the parent's extensible attribute is set to Not Inherited.</td>
</tr>
<tr>
<td>Disabled</td>
<td>Extensible attribute inheritance is not enabled for the attribute.</td>
</tr>
<tr>
<td>No Change</td>
<td>The extensible attributes of the selected objects do not have the same inheritance state for all objects. This state allows you to retain the current state on the selected objects. Note that this state is only seen in the Multi-object Extensible Attributes editor.</td>
</tr>
</tbody>
</table>

When you add an inheritable extensible attribute to an object, if there are descendants of this object the Descendant Actions dialog box is displayed which will provide options for the descendants. Following is a summary of these options:

- Retain the original value of the attribute for all descendants.
- Inherit the extensible attribute and its value from the parent object.
- Inherit the extensible attribute and its value when it does not exist on descendants.
- If the extensible attribute does not exist on the descendant, do not add it.
- If you are deleting an inherited extensible attribute from a parent object you can retain or remove the extensible attribute from the object's descendants.

To configure default descendant actions for inheritable extensible attributes:

1. From the Grid tab, select the Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit.
2. In the Extensible Attribute Inheritance tab, complete the following:
   - When adding an extensible attribute that already exists on a descendant:
     - **Keep the descendant's existing value and change the inheritance state to Override:** Select this if you want to retain the existing extensible attribute values for all direct descendants, irrespective of the values you define at the parent level. The inheritance state for all direct descendants will be set to Overridden. Note that this is applicable only when you add a new extensible attribute to the parent object that already exists on the descendant. If you modify the value of an existing extensible attribute that is already inherited by the descendant, and select the above option in the Descendant Actions dialog box, then the new value will be inherited by the descendant, but the inheritance state will remain Inherited. For example, consider a network 10.0.0.0/16 that has an extensible attribute Site with the value SA (native). When you add another network 10.0.0.0/24, extensible attribute Site inherits its value, SA, from the parent object. Now, if you add network 10.0.0.0/8, assign extensible attribute Site and set its value to NY, then when you choose this option, the value of Site will remain as SA, but the inheritance state will be changed to Overridden for network 10.0.0.0/16; however, network 10.0.0.0/24 will still have its value as SA for Site with the inheritance state set to Inherited.
     - **Inherit the parent's value and change the inheritance state to Inherit:** Select this to inherit the extensible attribute values from the parent for all descendants. The inheritance state for all descendants will be set to Inherited.
     - **Change the inheritance state to Inherit only if the descendant's value is the same as the parent's value.** Otherwise, change the state to Override: Select this to set the inheritance state to Inherit if the descendants have the same extensible attribute value as the parent. Otherwise, retain the original extensible attribute value on the descendants and change the inheritance state to Overridden.

When adding an extensible attribute that does not exist on a descendant:

- Do not inherit the value from the parent and change the inheritance state to Not Inherited: Select this if the extensible attributes do not exist on the descendants and you do not want them to inherit the attributes from the parent. The inheritance state is set to Not Inherited.
- Inherit the value from the parent and change the inheritance state to Inherited: Select this if you want all descendants to inherit extensible attributes from the parent, and the inheritance state for all descendants will be set to Inherited.

When deleting an extensible attribute:

- **Keep the descendant's value and change the inheritance state to No Parent:** Select this if you want to preserve extensible attributes on all descendants when you delete an inheritable extensible attribute. The inheritance state for direct descendants will be set to No Parent.
- **If the current inheritance state is Inherited, remove the extensible attribute. If the current inheritance state is Overridden, keep the value and change the inheritance state to No Parent:** Select this if you want to remove the extensible attributes that are inherited.
For more information about how to configure inheritable extensible attributes, see Configuration Examples for Inheritable Extensible Attributes.

Admin Permissions and Inheritable Extensible Attributes

Permissions for descendant objects can affect the results of the actions that are chosen in the Descendant Actions dialog box:

- When you add an extensible attribute to the parent object: The descendants to which you have read-write permission will behave as expected with any of the chosen options in the Descendant Actions dialog box.
- When you change the extensible attribute value on the parent object: The descendants that have the same extensible attribute set to Inherited will be automatically changed to the new value, even though you may not have write permission for those descendants.
- When you select to preserve descendant values while removing an extensible attribute associated with the parent object, values will be preserved even if you do not have write-read permission for those descendants.
- When you select to remove an extensible attribute on descendants when removing a parent's extensible attribute, an error message will be displayed if you do not have write-read permission to some of the descendants.

Guidelines for Configuring Inheritable Extensible Attributes

- When you add an inheritable extensible attribute to a parent object, you can choose to have descendants inherit or override the parent's extensible attribute value. You can also choose that the extensible attribute not be added to a descendant.
- When you add a new parent with an inheritable extensible attribute, the options for changes to descendants remain the same as when you add a new inheritable extensible attribute to a parent. For more information, see Configuring Inheritable Extensible Attributes.
- When you add a new descendant to the existing parent with inheritable attributes, the descendant inherits all the extensible attributes. However, you can select if you want to inherit or override the values. If you set the inheritance state to Not Inherited, then the extensible attribute will not exist on the descendant, but you can later change the state to Inherited or Overridden. For more information, see Managing Inheritable Extensible Attributes at the Parent and Descendant Level.
- When you delete an inheritable extensible attribute associated with the parent, you can either preserve the extensible attribute values on the descendants or delete the inheritable extensible attributes. For information, see Deleting Inheritable Extensible Attributes Associated with Parent Objects.
- When you delete a parent object and if there is a grandparent, then the extensible attribute will be re-parented when you choose preserve. The current inheritance state of the attribute will be retained. If you delete a parent object and if there is no grandparent, then the inheritance state of the extensible attribute is changed to No Parent when you choose preserve.
- When you split a network, the extensible attribute will be copied to the newly created networks. For inheritable extensible attributes, the newly created network inherits the extensible attributes and the state is set to Inherited. For information, see Managing Inheritable Extensible Attributes at the Parent and Descendant Level.
- When you join two networks to form a larger network, the Descendant Actions dialog box is displayed with the following options:
  - **When joining networks**, select the action(s) you want to apply to the merged networks:
    - **Preserve extensible attributes for all descendants of the merged networks and change the inheritance state to No Parent**: Select this if you want to preserve the extensible attributes for all descendants of the merged networks. The inheritance state of the attributes will be changed to No Parent.
    - **Remove extensible attributes from descendants of the merged networks**: Select this if you want to remove extensible attributes that are inherited by descendants.

  **Note**: The options above apply only to extensible attributes which no longer have a parent, due to the merge. If the extensible attributes on descendants are also on the resulting merged network, then they will retain their current state.

When you add multiple inheritable networks, new networks will automatically inherit all extensible attributes from the parent.

Managing Inheritable Extensible Attributes at the Parent and Descendant Level

You can define if descendants will inherit values from the parent when a new extensible attribute is added to the parent. You can also choose to override the values of the extensible attributes on the descendants.

When you delete an existing attribute, you can choose to either preserve the values at the descendant level or delete the values inherited by the descendants.

**Note**: The Descendant Actions dialog box is displayed only when an object has descendants and you are modifying extensible attributes that affects those descendants. However, the dialog box is always displayed when a join is performed for a network that has inheritable extensible attributes.

The following section describes configuration changes for inheritable extensible attributes:

1. **Network Container**: From the Dashboards tab, select the Tasks tab -> click Add Networks. Select a network, enter the required details. You can edit the inheritable extensible attributes that are displayed automatically. If this is a parent object, then you can add extensible attributes.
   **IPv4 Network**: From the Data Management tab -> select the DHCP tab -> Networks tab. In the Networks section, select IPv4 Network from the Add drop-down menu. In the Add IPv4 Network wizard, enter the attributes in the Extensible Attributes tab after specifying the
required details.

**IPv6 Network:** From the Data Management tab -> select the DHCP tab -> Networks tab. In the Networks section, select IPv6 Network from the Add drop-down menu. In the Add IPv6 Network wizard, enter the attributes in the Extensible Attributes tab after specifying the required details.

**IPv4 Range:** From the Data Management tab > select the DHCP tab -> Networks tab -> Networks tab -> network > click addr_range, select Range from the Add drop-down menu. In the Add IPv4 Range wizard, enter the attributes in the Extensible Attributes tab after specifying the required details.

**IPv6 Range:** From the Data Management tab > select the DHCP tab -> Networks tab -> Networks tab -> network > click addr_range, select Range from the Add drop-down menu. In the Add IPv6 Range wizard, enter the attributes in the Extensible Attributes tab after specifying the required details.

2. You can either add new extensible attributes to the parent object or modify original extensible attribute values. Click on the extensible attribute value displayed in the Value column of the respective attribute to modify the original value or click the Add icon to add a new attribute.

3. Select a state from the drop-down list displayed in the Inheritance State column. Note that you can only change the inheritance state of a descendant. You must select Overridden from the drop-down list to enter a new value. For more information about inheritance states, see Table 8.2. When an object has a parent and the parent does not have the object's inheritable extensible attribute, then the inheritance state of the extensible attribute is set to No Parent and the state cannot be changed.

4. **Select the inheritable extensible attributes for which you want to modify descendant actions:** Select this check box if you would like to apply the actions of the Descendant Actions dialog box for existing extensible attributes. Before you select this check box, you must select the extensible attributes which will be affected by the actions of the Descendant Actions dialog box.

   **Note:** This check box is not displayed for hosts, fixed addresses, and reservations since they do not have descendants.

5. In the Descendant Actions dialog box, select options that will be applied for descendant objects as described in Configuring Inheritable Extensible Attributes.

   The Descendant Actions dialog box displays all the mentioned options when you perform add and delete operations simultaneously. Consider an example where you add a new inheritable extensible attribute Site, and delete an existing inheritable attribute Region from the parent object, and then click Save to save both changes. In this case, the Descendant Actions dialog box displays all the options.

6. Save the configuration.

### Viewing Extensible Attributes

To view the configured extensible attributes, from the Administration tab, select the Extensible Attributes tab. The panel displays the following information:

- **Name:** The name of the extensible attribute.
- **Type:** The type of data defined by the attribute.
- **Comment:** Comments entered for the extensible attribute.
- **Required:** Indicates whether users are required to complete this field.
- **Restricted to Objects:** The object types that are associated with the attribute.
- **Inheritance Enabled:** Indicates whether inheritance is enabled or not. You can do the following in this panel:
  - Sort the displayed data in ascending or descending order by column.
  - Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
  - Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
  - Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
  - Group results by extensible attributes. For information, see Grouping Results by Extensible Attributes.
  - Add or delete extensible attributes.
  - Print or export the data.

### Modifying Extensible Attributes

When you modify an extensible attribute, all objects using the modified attributes are updated. You can perform inline editing by double-clicking the row of data that you want to modify. The appliance displays the inline editing editor in the selected row. Click Save after modifying the data. Note that you cannot edit extensible attributes that have multiple values.

To modify an extensible attribute:

1. In the Administration tab, select the Extensible Attributes tab.
2. Select the attribute and click the Edit icon.
3. In the General tab of the Extensible Attributes editor, you can only change the name of the attribute. You cannot change the data type. The data type for predefined attributes is string.
4. In the Additional Properties tab, you can modify any of the fields described in step 4 of Adding Extensible Attributes.
5. Save the configuration and click Restart if it appears at the top of the screen.

### Modifying Inheritable Extensible Attributes

When values are inherited by a descendant, the inheritance state of the inherited extensible attribute is displayed as Inherited. You can select Ov
erridden and specify a new value or select Inherited to retain the same value as the parent. If you select Not Inherited, the extensible attribute and its value will not be inherited. The inherited value will have a strike-through and you cannot edit the value when the state is set to Not Inherited.

In addition to the attribute values, the Value column of an inheritable extensible attribute also displays the name of the source and the object type of the extensible attribute. For example, a Network Container has a descendant, Network, which inherits an extensible attribute value from Network Container and Network has a descendant, Fixed Address that inherits the same extensible attribute value. In this case, Fixed Address shows Network Container as the source.

The following table displays various inheritance states and corresponding changes to source and object types that are displayed in the Value column of an extensible attribute.

<table>
<thead>
<tr>
<th>Inheritance State</th>
<th>Source and Object Type in the Value Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>If an extensible attribute is a native attribute (an object which is at the top of the inheritance chain, or does not have ancestors),</td>
<td>Source is not displayed in the Value column. This column will not display the source details, if none of the selected objects support inheritance.</td>
</tr>
<tr>
<td>If the state of an extensible attribute is set to Inherited,</td>
<td>then the Source and object is displayed. You cannot change the value of the extensible attribute.</td>
</tr>
<tr>
<td>If the state of an extensible attribute is set to Overridden or Not Inherited,</td>
<td>then the Source will have a strike-through. You can change the state of such extensible attributes. You cannot change the value of the extensible attribute when the inheritance state is set to Not Inherited.</td>
</tr>
</tbody>
</table>

To modify the value and inheritance state of an inheritable extensible attribute:

1. For IPv4 and IPv6 Network: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks network -> addr_range check box, and then click the Edit icon.
   For IPv4 Range, IPv6 Range, Fixed Address, Reservation, and Host: From the Data Management tab > select the DHCP tab -> Networks tab -> network -> click addr_range, click the Edit icon.
2. In the editor, click the Extensible Attributes tab, select the check box of the respective attribute.
3. At the parent level, click on the value you want to change and enter the new value.
   At the descendant level, click on the value you want to change and enter the new value. Note that you can change the value only when the inheritance state is set to Overridden.
4. Select a state from the drop-down list displayed in the Inheritance State column. Note that you can only change the inheritance state of a descendant. You must select Overridden from the drop-down list to enter a new value. For more information, see Table 8.2.
5. Select the inheritable extensible attributes for which you want to modify descendant actions: Select this check box if you would like to apply the actions of the Descendant Actions dialog box for existing extensible attributes. Before you select this check box, select the extensible attributes which will be affected by the actions of the Descendant Actions dialog box. For more information about the Descendant Actions dialog box, see Managing Inheritable Extensible Attributes at the Parent and Descendant Level.
6. Save the configuration.

Deleting Extensible Attributes

When you delete an extensible attribute, the appliance removes the attribute. All the attribute values set on the selected object types are removed from those objects. Once deleted, the attribute no longer exists in the system. Deleted attributes are not moved to the Recycle Bin. This operation might take a long time depending on the amount of data that needs to be deleted.

To delete extensible attributes:

1. In the Administration tab, select the Extensible Attributes tab.
2. Select the attribute and click the Delete icon.
3. When the confirmation dialog box appears, click Yes.

Deleting Inheritable Extensible Attributes Associated with Parent Objects

When you remove an inheritable extensible attribute, which is associated with a parent object, you can choose to retain the descendant extensible attribute or remove it from all the descendants.

Note that you cannot delete extensible attributes that have the inheritance state set to Overridden, Inherited, and Not Inherited. You can delete an extensible attribute that is directly assigned to the object and has its inheritance state set to No Parent or if the inheritance state is Disabled.

To remove an inheritable extensible attribute associated with a parent object:

1. IPv4 and IPv6 Network: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.
   For IPv4 Range, IPv6 Range, Fixed Address, Reservation, and Host: From the Data Management tab DHCP -> tab -> Networks tab -> network -> click addr_range, select the object and click Edit icon.
2. In the editor, click the Extensible Attributes tab, select the attributes and then click the Delete icon.
3. When you click Save and Close, the Descendant Actions dialog box is displayed automatically with the following options:
   Select the action(s) you want to apply to descendant objects that have the following extensible attribute(s):
   When deleting an extensible attribute:
• Keep the descendant’s value and change the inheritance state to No Parent: Select this if you want to preserve extensible attributes for all descendants. The inheritance state of the extensible attribute changes to No Parent.

• If the current inheritance state is Inherited, remove the extensible attribute. If the current inheritance state is Overridden, keep the value and change the inheritance state to No Parent: Select this if you want to remove the extensible attributes that are inherited by the descendants. If the inheritance state of the extensible attributes is set to Inherited on the descendant, the attributes will be removed; however, if the inheritance state is set to Overridden, then the state will be changed to No Parent.

4. Click Yes to save the configuration or No to exit.

Note: The deleted extensible attributes will not be moved to the Recycle Bin and you cannot restore extensible attributes that are deleted.

Using Extensible Attributes

After a superuser admin configures the attributes of an object, they become available in the wizard and editor of the object. This section describes how users can then add and manage the attributes that were configured.

Grid Manager displays the required extensible attributes in the Extensible Attribute tab. You must enter values for all required attributes. If an object does not have required attributes, you can add the available optional attributes.

In the Extensible Attribute tab of an object, such as a network or host record, you can do the following:

• Enter values for extensible attributes
• Add attributes
• Change the inheritance state of an extensible attribute
• Select if descendants must inherit extensible attribute values from its parent
• Delete optional attributes

To enter values for the extensible attributes of an object:

1. Open the editor of the object. For example, to enter values for the attributes of a network, select it and click its Extensible Attributes tab.
2. Click the Value column of the attribute. You must enter values for all required attributes.
3. Depending on the required attribute type, either enter or select a value for the attribute from the Value column.
4. Based on whether the attribute is inheritable, the values are displayed in the Inheritance State column. This value can be set to Inherited, Overridden, or Not inherited. If the object is at the top of the inheritance chain (Network View), then the inheritance state is not displayed. The inheritance state is set to No Parent only if an object has a parent, but the parent does not have the inherited extensible attribute. This column is not displayed if all selected objects do not belong to the supported inheritance chain. Example: Zones, DNS View, DNS records, etc.

To add attributes:

1. Click the Add icon. Grid Manager adds a row to the table with the default attribute displayed.
2. Click the default attribute and expand the list of available attributes.
3. Select an attribute from the drop-down list.
4. Enter or select a value for the attribute from the Value column. To delete an attribute:
5. Click the check box beside the attribute you want to delete.
6. Click the Delete icon.

Note: You cannot delete an extensible attribute which has its inheritance state set to Inherited, Overridden, and Not Inherited. You can delete an extensible attribute that is directly assigned to the object and has its inheritance state set to No Parent or if the inheritance state is Disabled.

To delete all attributes:

1. Click the Attribute Name check box.
2. Click the Delete icon.

Note: You can delete only attributes that are not required. If you have one or more required attributes, you cannot use the delete all function.

3. Save the configuration and click Restart if it appears at the top of the screen.

Editing Multiple Extensible Attribute Values

You can also manage the extensible attributes of multiple objects at the same time. For example, you can select several zones, and view and modify their extensible attributes all at once in the Multi-Select Edit Extensible Attributes editor.

Note that Grid Manager may not apply the changes you made to all the selected objects. It applies the change to objects that meet the following criteria:

• You have read/write permission to the object.
• The selected object is not locked by another user or does not have a scheduled pending task.
• If the attribute was restricted to certain object types, the object must be one of those types. To edit multiple extensible attribute values:
1. Select the objects whose extensible attributes you want to modify. You can select specific objects or select all objects in a dataset, as described in Selecting Objects in Tables.

2. Expand the Toolbar and click Extensible Attributes. Grid Manager displays the Multi-Select Edit Extensible Attributes dialog box which lists the extensible attributes of the selected objects. It displays the following information for each attribute:

- **Attribute Name**: This field displays the name of the extensible attribute associated with the selected object.
- **Value**: If the selected objects have the same value for the attribute, Grid Manager displays that value in this field. If the selected objects have different values for the attribute or if some have values and others do not, this field displays Multiple Values and the cell is highlighted in gray. An attribute can have multiple rows if it allows multiple values. Grid Manager displays the values that all objects have in common, if any. Otherwise, it displays Multiple Values. This column displays the source for inherited extensible attributes only. Note that when you add new extensible attributes, edit values of existing extensible attributes or delete an extensible attribute, then the Descendant Actions dialog box is displayed, even if the objects do not have any descendants. For more information about Source values, see Modifying Inheritable Extensible Attributes.
- **Inheritance State**: This field displays the inheritance state of an extensible attribute. The column value can be Inherited, Not Inherited, No Parent, No Change or Overridden. This column is not displayed if all selected objects do not belong to the supported inheritance chain. Example: Zones, DNS View, DNS records, etc.
- **Required**: This field displays Yes if the attribute is required in at least one object associated with the attribute. It displays No if the attribute is not required in any of the objects.

3. You can do the following:
   - Change the value of an attribute. Depending on the attribute type, select the value and either enter a new value or select one from the drop-down list.
   - Add an attribute to the selected objects. Click the Add icon. In the Attribute Name field of the new row, select an attribute from the list of available attributes and specify its value. If the attribute that you added was configured as a required attribute, the Required field displays Yes. Otherwise, it displays No.
   - Delete an attribute. You can delete an attribute if it is not required. Select the attribute and click the Delete icon.

4. Click OK when you are finished modifying the extensible attributes.

Grid Manager applies your changes to the applicable objects. This operation might take a long time, depending on the amount of data being modified. You can choose to run this operation in the background, as described in About Tasks.

### Grouping Results by Extensible Attributes

You can enable the appliance to group members and services with the same extensible attributes. Grid Manager displayed group data with the same value for the specified extensible attribute. To group results by extensible attributes:

1. From the Grid tab, select the Grid Manager tab -> Members tab or Services tab.
   
   From the Data Management tab, select the DHCP or DNS tab -> Members/Servers tab.

2. Complete the following to group members with the same extensible attribute:
   - **Group Results**: Select this check box to enable the appliance to group members by extensible attributes.
   - **Group By**: Select an extensible attribute by which you want to group members from the drop-down list. Grid Manager displays data per group of members configured with the same extensible attribute value.
     
     To add additional Group By filter, click the + icon, and then select a value from the drop-down list. You can apply up to 10 Group By filters. You can also delete a filter by clicking the - icon.

### Configuration Examples for Inheritable Extensible Attributes

All examples in this section are based on the inheritance chain Network View -> Network Container -> Network -> Range -> Host/Fixed Address/Reservation, in which network view is at the top level and host, fixed address and reservation at the bottom of the inheritance chain.

#### Example 1

When you add an extensible attribute to the top object, the inheritance state is set to No Parent. For example, if you add a new inheritable extensible attribute, Building, to a network view, the inheritance state of this extensible attribute is set to No Parent for the network view.
Example 2

When you add an extensible attribute Site to the parent object Network that has a descendant Range, you can define Site as inheritable and add it to the Network. The descendant, Range, may or may not have the same extensible attribute. Infoblox displays a list of options that lets you either inherit the value or retain or override the existing value of the extensible attribute at the descendant level. Another option is to inherit the value of Site, only if the value for this attribute in Range is same as that in Network. You can also decide if Range should acquire the same value for Site, if it is not defined for Range. This change can be inherited by the descendants of Range.

Depending on your configuration, the inheritance state of the extensible attribute can display Inherited, Overridden or Not Inherited. If the object is at the top of the inheritance chain (Network View), then the inheritance state is not displayed. The inheritance state is set to No Parent only if an object has a parent, but the parent does not have the inherited extensible attribute.

Example 3

Examples in this section show different results when you add a new inheritable extensible attribute to an object located at the top or in the middle of the inheritance chain based on the following:

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Network</td>
<td>Region</td>
<td>ABC</td>
<td></td>
</tr>
<tr>
<td>10.1.0.0/16</td>
<td>Network</td>
<td></td>
<td></td>
<td>Native</td>
</tr>
</tbody>
</table>

Example 3.1: Add an extensible attribute Region with value DEF to 10.0.0.0/8

You select the following options for the existing extensible attribute:

- For descendants that already have this extensible attribute, the existing extensible attribute will always be set to Inherit.
- For descendants that do not have this extensible attribute, the descendants will inherit this extensible attribute.

Result:

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Region</td>
<td>DEF</td>
<td>Native</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Network</td>
<td>Region</td>
<td>DEF</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
<tr>
<td>10.1.0.0/16</td>
<td>Network</td>
<td>Region</td>
<td>DEF</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
</tbody>
</table>

Example 3.2: Add an extensible attribute Region with value DEF to 10.0.0.0/8

You select the following options for the existing extensible attribute:

- For descendants that already have this extensible attribute, the existing extensible attribute will always be set to Override.
- For descendants that do not have this extensible attribute, the descendants will not inherit this extensible attribute (extensible attribute is set to Do not Inherit).

Result:

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Region</td>
<td>DEF</td>
<td>Native</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Network</td>
<td>Region</td>
<td>ABC</td>
<td>Overridden</td>
</tr>
<tr>
<td>10.1.0.0/16</td>
<td>Network</td>
<td>Region</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example 3.3: Add an extensible attribute Region with value DEF to 10.0.0.0/8

You select the following options for the existing extensible attributes:

- For descendants that already have this extensible attribute, the existing extensible attribute will always be set to Inherit.
- For descendants that do not have this extensible attribute, the descendants will not inherit this extensible attribute (extensible attribute is set to Do not Inherit).

Result:
Example 4

Examples in this section show different results when you remove an existing inheritable extensible attribute from an object located at the top or in the middle of the inheritance chain based on the following:

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Region</td>
<td>DEF</td>
<td>Native</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Network</td>
<td>Region</td>
<td>DEF</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
<tr>
<td>10.1.0.0/16</td>
<td>Network</td>
<td>Region</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example 4.1: Remove extensible attribute Region with value DEF from 10.0.0.0/8

You select the following option for the existing extensible attribute:

- Remove extensible attributes with inheritance state set to **Inherited**. Extensible attributes with the state set to **Overridden** are not removed.

Result:

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Region</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Network</td>
<td>Region</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.0.0/16</td>
<td>Network</td>
<td>Region</td>
<td>ABC</td>
<td>Overridden</td>
</tr>
</tbody>
</table>

Example 4.2: Remove extensible attribute Region with value DEF from 10.0.0.0/8 You select the following option for the existing extensible attribute:

- Preserve all descendant extensible attributes, whether the state is set to **Inherited** or **Overridden**. Result:

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Region</td>
<td>DEF</td>
<td>Native</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Network</td>
<td>Region</td>
<td>DEF</td>
<td>Native</td>
</tr>
<tr>
<td>10.1.0.0/16</td>
<td>Network</td>
<td>Region</td>
<td>ABC</td>
<td>Native</td>
</tr>
</tbody>
</table>

Example 5

Examples in this section show different results when you remove parent object based on the following:

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Region</td>
<td>DEF</td>
<td>Native</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Network Container</td>
<td>Region</td>
<td>DEF</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
<tr>
<td>10.1.0.0/24</td>
<td>Network</td>
<td>Region</td>
<td>DEF</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
<tr>
<td>10.1.0.0/24</td>
<td>Network</td>
<td>Region</td>
<td>ABC</td>
<td>Overridden</td>
</tr>
<tr>
<td>10.10.0.0/16</td>
<td>Network Container</td>
<td>Region</td>
<td>GHI</td>
<td>Overriden</td>
</tr>
<tr>
<td>10.10.0.0/24</td>
<td>Network</td>
<td>Region</td>
<td>GHI</td>
<td>Inherited from 10.10.0.0/16</td>
</tr>
</tbody>
</table>
Example 5.1: Removing 10.0.0.0/8 from the parent level
You select the following option for the existing extensible attribute:

- Remove extensible attributes with the inheritance state set to **Inherited**. Extensible attributes with the state set to **Overridden** are not removed.

Result:

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>Network Container</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.0.0/24</td>
<td>Network</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.1.0/24</td>
<td>Network</td>
<td>Region</td>
<td>ABC</td>
<td>Overridden</td>
</tr>
<tr>
<td>10.10.0.0/16</td>
<td>Network Container</td>
<td>Region</td>
<td>GHI</td>
<td>Overridden</td>
</tr>
<tr>
<td>10.10.0.0/24</td>
<td>Network</td>
<td>Region</td>
<td>GHI</td>
<td>Inherited from 10.10.0.0/16</td>
</tr>
<tr>
<td>10.10.1.0/24</td>
<td>Network</td>
<td>Region</td>
<td>JKL</td>
<td>Overridden</td>
</tr>
</tbody>
</table>

Example 5.2: Removing object 10.0.0.0/8 from the parent level
You select the following option for the existing extensible attribute on descendants:

- Preserve all extensible attributes on the descendant.

Result:

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>Network Container</td>
<td>Region</td>
<td>DEF</td>
<td>Native</td>
</tr>
<tr>
<td>10.0.0.0/24</td>
<td>Network</td>
<td>Region</td>
<td>DEF</td>
<td>Inherited from 10.0.0.0/16</td>
</tr>
<tr>
<td>10.0.1.0/24</td>
<td>Network</td>
<td>Region</td>
<td>ABC</td>
<td>Overridden</td>
</tr>
<tr>
<td>10.10.0.0/16</td>
<td>Network Container</td>
<td>Region</td>
<td>GHI</td>
<td>Native</td>
</tr>
<tr>
<td>10.10.0.0/24</td>
<td>Network</td>
<td>Region</td>
<td>GHI</td>
<td>Inherited from 10.10.0.0/16</td>
</tr>
<tr>
<td>10.10.1.0/24</td>
<td>Network</td>
<td>Region</td>
<td>JKL</td>
<td>Overridden</td>
</tr>
</tbody>
</table>

Example 5.3: Remove object 10.10.0.0/16 from the parent level
You select the following option for the existing extensible attribute on descendants:

- Remove extensible attributes with the inheritance state set to **Inherited**. Extensible attributes with the state set to **Overridden** are retained.

Result:

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Region</td>
<td>DEF</td>
<td>Native</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Network Container</td>
<td>Region</td>
<td>DEF</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
<tr>
<td>10.0.0.0/24</td>
<td>Network</td>
<td>Region</td>
<td>DEF</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
<tr>
<td>10.0.1.0/24</td>
<td>Network</td>
<td>Region</td>
<td>ABC</td>
<td>Overridden</td>
</tr>
<tr>
<td>10.10.0.0/24</td>
<td>Network</td>
<td>Region</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.1.0/24</td>
<td>Network</td>
<td>Region</td>
<td>JKL</td>
<td>Overridden</td>
</tr>
</tbody>
</table>

Example 6
Examples in this section show different results after you add an object in the middle of the inheritance chain based on the following:
Example 6.1: Adding object 10.10.0.0/16 without extensible attributes You select the following option for the existing extensible attribute:

- Retain values if the extensible attribute already exists, and inherit the attribute from the parent object if it does not exist.

Result:

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Owner</td>
<td>Admin</td>
<td>Native</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Network Container</td>
<td>Owner</td>
<td>Admin</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
<tr>
<td>10.0.0.0/24</td>
<td>Network</td>
<td>Owner</td>
<td>Admin</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
<tr>
<td>10.0.1.0/24</td>
<td>Network</td>
<td>Owner</td>
<td>Joe</td>
<td>Overridden</td>
</tr>
<tr>
<td>10.10.0.0/16</td>
<td>Network Container</td>
<td>Owner</td>
<td>Admin</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
<tr>
<td>10.10.0.0/24</td>
<td>Network</td>
<td>Owner</td>
<td>Admin</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
<tr>
<td>10.10.1.0/24</td>
<td>Network</td>
<td>Owner</td>
<td>Annie</td>
<td>Overridden</td>
</tr>
</tbody>
</table>

Example 7

Examples in this section show different results after you modify inheritable extensible attributes with multiple values based on the following:

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Region</td>
<td>MNO</td>
<td>Native</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Network Container</td>
<td>Region</td>
<td>PQR</td>
<td>Native</td>
</tr>
</tbody>
</table>

Example 7.1: Adding extensible attribute Region with value GHI to 10.0.0.0/8 You select the following option for the existing extensible attributes:

- The descendants that already have this extensible attribute will inherit the value from the parent object.

Result: Multiple values will be replaced with the single inherited value.

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Region</td>
<td>GHI</td>
<td>Native</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Network Container</td>
<td>Region</td>
<td>GHI</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
</tbody>
</table>

Example 7.2: Adding extensible attribute Region with value GHI to 10.0.0.0/8 You select the following option for the existing extensible attributes:

- The descendants that already have this extensible attribute will override the value.

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Region</td>
<td>GHI</td>
<td>Native</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Network</td>
<td>Region</td>
<td>DEF</td>
<td>Overridden</td>
</tr>
</tbody>
</table>

Example 8

Examples in this section show different results after you modify existing inheritable extensible attribute of an object, but you do not have required permission to modify some descendants. For information about admin permissions, see About Administrative Permissions.
<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Owner</td>
<td>Sam</td>
<td>Native</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Network Container</td>
<td>Owner</td>
<td>Sam</td>
<td>Inherited from</td>
</tr>
<tr>
<td>10.0.0.0/24</td>
<td>Network</td>
<td>Owner</td>
<td>Sam</td>
<td>Inherited from</td>
</tr>
<tr>
<td>10.0.1.0/24</td>
<td>Network</td>
<td>Owner</td>
<td>Bob</td>
<td>Overridden</td>
</tr>
<tr>
<td>10.10.0.0/16</td>
<td>Network Container</td>
<td>Owner</td>
<td>John</td>
<td>Inherited from</td>
</tr>
<tr>
<td>10.10.1.0/24</td>
<td>Network</td>
<td>Owner</td>
<td>Max</td>
<td>Overridden</td>
</tr>
<tr>
<td>10.20.0.0/16</td>
<td>Network Container</td>
<td>Owner</td>
<td>Sam</td>
<td>Inherited from</td>
</tr>
<tr>
<td>10.20.0.0/24</td>
<td>Network</td>
<td>Owner</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.0/24</td>
<td>Network</td>
<td>Owner</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example 8.1: Removing object 10.0.0.0/8**

You select the following option for the existing inheritable extensible attribute:

- Retain extensible attribute values on descendants that are inherited from this parent object.

**Result:**

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>Network Container</td>
<td>Owner</td>
<td>Sam</td>
<td>Native</td>
<td>Read</td>
</tr>
<tr>
<td>10.0.0.0/24</td>
<td>Network</td>
<td>Owner</td>
<td>Sam</td>
<td>Native</td>
<td>Read</td>
</tr>
<tr>
<td>10.0.1.0/24</td>
<td>Network</td>
<td>Owner</td>
<td>Bob</td>
<td>Overridden</td>
<td>Write</td>
</tr>
<tr>
<td>10.10.0.0/16</td>
<td>Network Container</td>
<td>Owner</td>
<td>John</td>
<td>Overridden</td>
<td>Read</td>
</tr>
<tr>
<td>10.10.1.0/24</td>
<td>Network</td>
<td>Owner</td>
<td>Max</td>
<td>Overridden</td>
<td>Read</td>
</tr>
<tr>
<td>10.20.0.0/16</td>
<td>Network Container</td>
<td>Owner</td>
<td>Sam</td>
<td>Inherited from 10.10.0.0/16</td>
<td>Read</td>
</tr>
<tr>
<td>10.20.0.0/24</td>
<td>Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.0/24</td>
<td>Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example 8.2: Removing object 10.0.0.0/8**

You select the following option for the existing inheritable extensible attribute:

- Remove extensible attribute values from descendants that are inherited from this parent object.

The appliance displays an error message when you remove an extensible attribute that is associated with a descendant for which you do not have required permission.

**Result:**

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>Network Container</td>
<td></td>
<td></td>
<td></td>
<td>Read</td>
</tr>
</tbody>
</table>
Example 9

Examples in this section show different results after you join multiple networks, based on the following:

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.0.0/16</td>
<td>Network</td>
<td>Owner</td>
<td>John</td>
<td>Native</td>
</tr>
<tr>
<td>10.1.0.1</td>
<td>Fixed Address</td>
<td>Owner</td>
<td>John</td>
<td>Inherited from 10.1.0.0/16</td>
</tr>
<tr>
<td>10.2.0.0/16</td>
<td>Network</td>
<td>Owner</td>
<td>Sam</td>
<td>Native</td>
</tr>
<tr>
<td>10.2.0.1</td>
<td>Fixed Address</td>
<td>Owner</td>
<td>Jane</td>
<td>Overridden</td>
</tr>
</tbody>
</table>

**Example 9.1: Joining networks 10.0.0.0/8 with 10.1.0.0/16**

You select the following option for the existing extensible attribute:

- Join networks 10.0.0.0/8 with 10.1.0.0/16.

**Result:**

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Owner</td>
<td>John</td>
<td>Native</td>
</tr>
<tr>
<td>10.1.0.1</td>
<td>Fixed Address</td>
<td>Owner</td>
<td>John</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
<tr>
<td>10.2.0.1</td>
<td>Fixed Address</td>
<td>Owner</td>
<td>Jane</td>
<td>Overridden</td>
</tr>
</tbody>
</table>

**Example 9.2: Joining networks 10.0.0.0/8 with 10.2.0.0/16**

You select the following option for the existing extensible attribute:

- Join networks 10.0.0.0/8 with 10.2.0.0/16.

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Extensible Attribute</th>
<th>Extensible Attribute Value</th>
<th>Inheritance State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Network Container</td>
<td>Owner</td>
<td>Sam</td>
<td>Native</td>
</tr>
<tr>
<td>10.1.0.1</td>
<td>Fixed Address</td>
<td>Owner</td>
<td>Sam</td>
<td>Inherited from 10.0.0.0/8</td>
</tr>
<tr>
<td>10.2.0.1</td>
<td>Fixed Address</td>
<td>Owner</td>
<td>Jane</td>
<td>Overridden</td>
</tr>
</tbody>
</table>

**Managing Security Operations**

The Grid provides certain security-related features. The following sections describe the different security-related features that you can set.

**Restricting Remote Console Access**

You can restrict admins from accessing the Infoblox CLI from a remote location using an SSH (Secure Shell) v2 client. When you select this only
admins who have access rights will be able to access the Infoblox CLI using an SSH (Secure Shell) v2 client. By default, this option is disabled.

Restricting GUI/API Access

You can specify the IP addresses from which administrators are allowed to access the NIOS appliance. When the NIOS appliance receives a connection request, it tries to match the source IP address in the request with IP addresses in the list. If there is at least one item in the HTTP Access Control list and the source IP address in the request does not match it, the NIOS appliance ignores the request.

Caution: If you specify an address or network other than the one from which you are currently accessing the appliance, when you save your configuration, you will lose your administrative session and be unable to reconnect. If you have enabled the Enable GUI/API Access via both M GMT and LAN1/VIP feature and configured ACLs to control access to the GUI and API, then the same set of ACLs are applicable on both the interfaces (LAN1 and MGMT port). For information, see Enabling GUI and API Access on the MGMT and LAN1/VIP Ports and 5800922.

Enabling HTTP Redirection

You can enable the NIOS appliance to redirect administrative connection requests using HTTP to the secure HTTPS protocol. When you disable redirection, the NIOS appliance ignores any administrative connection requests not using HTTPS. By default, the NIOS appliance does not redirect HTTP connection requests to HTTPS. When you change this setting, the application restarts and your management session terminates.

Modifying the Session Timeout Setting

You can set the length of idle time before an administrative session to the Infoblox GUI times out. The default timeout value is 600 seconds (10 minutes).

If a user does not interact with the application for the specified time, the appliance displays a message that a timeout has occurred. Click OK to restart the GUI session.

Note: If you change the session timeout value, the new setting takes effect only after you log out and log back in.

Disabling the LCD Input Buttons

By default, the LCD input function is enabled, which allows you to use the LCD buttons on the front panel of a NIOS appliance to change the IPv4 address settings of the LAN port. You can disable this function if the appliance is in a location where you cannot restrict access exclusively to NIOS appliance administrators and you do not want anyone to be able to make changes through the LCD.

Configuring Security Features

You can manage only certain features at the member level. To configure security features for the Grid or an individual member:

1. Grid: From the Grid tab, select the Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit.

Member: From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.

To override an inherited property, click Override next to it and complete the appropriate fields.

1. In the Security tab, complete the following:
   - Session Timeout(s): This field is in the Grid Properties editor only. Enter a number between 60 and 31536000 seconds (one minute – one year) in the Session Timeout field. The default session timeout is 600 seconds (10 minutes).
   - Minimum Password Length: This field is in the Grid Properties editor only. Specify the minimum number of characters allowed for an admin password.
   - Redirect HTTP to HTTPS: This field is in the Grid Properties editor only. Select this option to have the appliance redirect HTTP connection requests to HTTPS.
   - Restrict GUI/API Access: To control access to the GUI and API, select one of the following. You can restrict access using a named ACL or define individual ACEs. For information about named ACLs, see Configuring Access Control.
     - Allow Any: Select this to allow any clients to access the GUI and API. This is selected by default.
     - Named ACL: Select this and click Select Named ACL to select a named ACL that contains only IPv4 and IPv6 addresses and networks. GUI and API access restriction does not support TSIG key based ACEs. When you select this, the appliance allows GUI and API access for all ACEs in the named ACL. You can click Clear to remove the selected named ACL.
     - Set of ACEs: Select this to configure individual access control entries (ACEs). Click the Add icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding.
       - IPv4 Address and IPv6 Address: Select this to add an IPv4 address or an IPv6 address. Click the Value field and enter the IP address. The appliance allows this client to access the GUI and API and restricts others.
         - IPv4 Network and IPv6 Network: Select this to add an IPv4 network or IPv6 network. Click the Value field and
enter the network. The appliance allows this network to access the GUI and API and restricts others. After you have added access control entries, you can do the following:

- Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL icon and enter a name in the Convert to Named ACL dialog box. The appliance creates a new named ACL and adds it to the Named ACL panel. Note that the ACEs you configure for this operation stay intact.
- Reorder the list of ACEs using the up and down arrows next to the table.
- Select an ACE and click the Delete icon to delete the entry. You can select multiple ACEs for deletion.

- **Access Restrictions Apply to Remote Console:** Select this to restrict admins from accessing the Infoblox CLI from a remote location using SSH (Secure Shell) v2 client.
- **Enable Remote Console Access:** Select this option to enable superuser admins to access the Infoblox CLI from a remote location using SSH (Secure Shell) v2 clients. You can set this at the Grid and member levels.
- **Enable Support Access:** Select this check box to enable an SSH (Secure Shell) daemon that only Infoblox Technical Support can access. You can set this at the Grid and member levels.
- **Restrict Remote Console and Support Access to the MGM T Port:** This field is in the Grid Member Properties editor only. Select this check box to restrict SSH (Secure Shell) v2 access to the MGMT port only. This restricts Infoblox Technical Support and remote console connections—both of which use SSH v2—to just the MGMT port. For an HA pair, you can make an SSH v2 connection to the MGMT port on both the active and passive node. Clear the check box to allow SSH v2 access to both the MGMT and LAN ports.
- **Permanently Disable Remote Console and Support Access:** This field is in the Grid Properties editor only. Select this option to permanently disable remote console (Secure Shell v2) access for appliance administration and for Infoblox Technical Support.
- **Enable LCD Input:** Select this check box to allow use of the LCD buttons on the front panel of a NIOS appliance to change the IP address settings of the LAN port. Clear this check box to disable this function. You can set this at the Grid and member levels.

2. Save the configuration and click **Restart** if it appears at the top of the screen.

### Enabling and Disabling Remote Console and Infoblox Technical Support Access

Infoblox Technical Support might need access to your NIOS appliance to troubleshoot problems. This function enables an SSH (Secure Shell) daemon that only Infoblox Technical Support can access. By default, this option is disabled. This function also makes it possible for a superuser admin to access the Infoblox CLI from a remote location using an SSH (Secure Shell) v2 client. The management system must have an SSH v2 client to use this function. After opening a remote console connection using an SSH client, log in using a superuser name and password. By default, this option is disabled. Note that only superusers can log in to the appliance through a console connection.

You can permanently disable remote console (Secure Shell v2) access for appliance administration and for Infoblox Technical Support to perform remote troubleshooting. Disabling this type of access might be required in a high-security environment.

---

**WARNING:** After permanently disabling remote console and support access, you cannot re-enable them! Not even resetting an appliance to its factory default settings can re-enable them.

---

If you have any questions, contact Infoblox Technical Support. To enable or disable remote console and Infoblox technical support access:

1. **Grid:** From the Grid tab, select the Grid Manager tab, expand the Toolbar and click **Grid Properties** -> **Edit**.
   - **Member:** From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.
   - **Independent appliance:** From the System tab, select the System Manager tab, expand the Toolbar and click **System Properties** -> **Edit**.
2. In the editor, select the Security tab -> **Advanced** tab, and then complete the following in the Remote Console and Infoblox Technical Support Access section:
   - **Enable Remote Console Access:** Select this check box to enable superuser admins to access the Infoblox CLI from a remote location using SSH (Secure Shell) v2 clients. You can set this at the Grid and member levels.
   - **Enable Support Access:** Select this check box to enable an SSH (Secure Shell) daemon that only Infoblox Technical Support can access. You can set this at the Grid and member levels.
   - **Support Access Info:** Displays the support access code and the expiration time of the code. Note that the **Enable Support Access** is disabled after the expiration time.
   - **Permanently Disable Remote Console and Support Access:** This field is in the Grid Properties editor only. Select this check box to permanently disable remote console (Secure Shell v2) access for appliance administration and for Infoblox Technical Support.
3. Save the configuration.

### Configuring Proxy Servers

If your network environment does not allow direct HTTP or HTTPS communication with the Internet through a firewall from a secure location in which the Grid Master or standalone appliance resides, you can configure your appliance to use a proxy server so you can receive automatic updates, such as threat protection rulesets and threat analytics bundles, through this connection. You can also configure a proxy server to perform AWS related communication, such as using a proxy server as the AWS API Proxy, performing vDiscovery on AWS endpoints, and pulling DNS data from Amazon Route 53. For information about AWS deployments, refer to the Installation Guide for vNIOSS for AWS. For information about vDiscovery, see Configuring vDiscovery Jobs.

**Note:** Note that configured proxy settings are for the entire Grid. You cannot configure proxy settings for individual members.
Depending on the updates you want to download, you may need to install the respective licenses in your Grid. For example, to download threat protection ruleset updates, the Grid must have the Threat Protection Update license installed. To download threat analytics bundles, you must install the Threat Analytics license. When you configure your appliance to obtain periodic ruleset updates, all updates go through the MGMT port on the Grid Master by default. You can, however, delegate this function to a Grid member using a different interface such as LAN1 or LAN2. For information about how to delegate updates to a Grid member and configure the interface, see 5800925 5800925.

To configure proxy settings for the Grid:

1. From the Grid tab, select the Grid Manager tab, and then click Edit -> Grid Properties from the Toolbar.
2. In the Grid Properties editor, select the Proxy Settings tab -> Basic tab, and complete the following:
   - Use Proxy Server: When you select this check box, the appliance uses the connection that has been established with the proxy server to establish connection with endpoints or download automatic updates, such as threat protection rulesets and threat analytics bundles. This setting applies to the entire Grid. When you clear this check box, the appliance does not use the proxy server; however, the configuration will not be affected.
   - Name or IP Address and Port: Enter the name or IP address and port number of the proxy server you plan to use for this connection.
   - HTTPS Proxy Content Inspection: From the drop-down list, select one of the following methods the proxy server uses to inspect packet content. Note that this section does not apply to AWS deployments.
     - None: Select this to use HTTP for the connection. This method does not allow certificate authentication for the proxy server.
     - Allow Deep Packet Inspection: This option is not supported for AWS deployments. To eliminate man-in-the-middle attacks, select this to allow deep packet inspection and information extraction for non-compliant protocol, intrusions, or other criteria that determine whether the packets should be routed to an alternate destination. When you select this, you must click Proxy Server Certificate and navigate to the proxy server certificate to upload it to the Grid, or you must ensure that a trusted chain has been established before the proxy server can perform deep packet inspection. When you have uploaded a certificate, the appliance displays Loaded.
     - Enable Strict Host Name Checking: This option is enabled only when you select Allow Deep Packet Inspection. As part of the SSL handshake process, the appliance verifies that the CN (Common Name) of the public certificate of the proxy server exactly matches the host name of the proxy server.

Credentials for Proxy Server (if configured at proxy server)

- Use username and password to connect to proxy server if configured: If you have configured user credentials on the proxy server, enter the Username and Password here. This is optional.

Configuring Members and Interfaces for Automatic Updates

If you want to download specific rulesets or updates from external servers, you can configure members and corresponding interfaces to receive updates automatically. Note that these members must have access to external servers from where the updates are delegated automatically. For a member to access an external server, you must specify the interface that you configure here when you set up an external server.

To delegate automatic updates to a Grid member or change the interface for downloads, complete the following:

1. From the Grid tab, select the Grid Manager tab, and then click Edit -> Grid Properties from the Toolbar.
2. In the Grid Properties editor, select the Proxy Settings tab -> Basic tab, and complete the following:
   - In the Members table, click the Add icon and select Add Member. In the Member Selector, select the member to which you want to delegate the automatic update function. The appliance adds the Grid member to the table. You can add up to five members for automatic updates. When you add multiple members, you can place the selected members in the order you prefer using the arrows next to the table. If for any reasons the first member is unable to receive updates, the appliance goes down the list in the order the members are placed until the next reachable member receives the updates.
   - Click the Interface column, and from the drop-down list select the interface (Any, LAN2, MGMT or VIP) you want the corresponding member to use for automatic updates. Ensure that the selected interface is configured properly on the member. The default is Any, which maps to the LAN1 interface for all appliance models, except for the PT models. For all PT appliances, Any maps to the MGMT interface. You can select MGMT or Any for threat protection members. Note that VLANs are not supported. You can click the Test connectivity to all members icon to ensure that the connectivity between the ruleset download web site and all Grid members is properly established using the selected interface. The appliance displays a message indicating the connectivity status in the feedback panel.
   - The table displays the following:
     - Name: Displays the member name. For the Grid Master, this field displays Grid Master.
     - Interface: Displays the selected interface that is used for automatic updates.

Note: The appliance generates an SNMP trap if any of the configured Grid members failed to receive updates.

Configuring Ethernet Ports

Depending on your deployment and configuration choices, the Ethernet ports on the NIOS appliance perform different functions. The Ethernet ports that handle traffic on the NIOS appliance are as follows:

- LAN1 port – A 10/100/1000-Mbps gigabit Ethernet port that connects the appliance to the network. This is the default port for single independent appliances, single Grid members, and passive nodes in HA pairs. You must use the LAN1 port to set up the appliance initially. It handles traffic for all management services if you do not enable the MGMT and LAN2 ports. The passive node in an HA pair...
LAN2 port – A 10/100/1000-Mbps gigabit Ethernet port that connects the appliance to the network. The LAN2 port is not enabled by default. You can enable the LAN2 port and define its use through the GUI after the initial setup. By default, the appliance uses the LAN1 port (and HA port when deployed in an HA pair). To enable and configure the LAN2 port, you must have read/write permission to the Grid member on which you want to enable the port. The LAN2 port is available on the TE-810, TE-820, TE-1410, TE-1420, TE-2210, TE-2220, and IB-4010 appliances. For information about how to use the LAN2 port, see Using the LAN2 Port.

• HA port – A 10/100/1000-Mbps gigabit Ethernet port through which the active node in an HA (high availability) pair connects to the network using a VIP (virtual IP) address. HA pair nodes also use their HA ports for VRRP (Virtual Router Redundancy Protocol) advertisements.

• MGMT port – A 10/100/1000-Mbps gigabit Ethernet port that you can use for appliance management or DNS service. You can enable the MGMT port and define its use through the GUI after the initial setup. If the MGMT port is enabled, the NIOS appliance uses it for management services (see bookmark906 for specific types).

You can do the following on some of the Ethernet ports, depending on your network requirements and configurations:

• Assign VLANs (Virtual LANs) to the LAN1 and LAN2 ports so that NIOS can provide DNS service to different subnetworks on the same interface. For more information about VLANs, see bookmark899.

• Implement DiffServ (Differentiated Services) on the appliance by configuring the DSCP (Differentiated Services Code Point) value. For more information about DiffServ and DSCP, see bookmark901 bookmark901.

Enabling GUI and API Access on the MGMT and LAN1/VIP Ports

You can access the Infoblox GUI and API through the MGMT and LAN1 or VIP interfaces simultaneously. To do so, you must first configure the MGMT port on the appliance, and then enable the Enable GUI/API Access via both MGMT and LAN1/VIP feature. For information about the MGMT port, see Using the MGMT Port. When you enable this feature, you can use the MGMT and LAN1 ports for standalone appliances and MGMT and VIP ports for an HA pair. This feature is disabled for all new installations and upgrades.

Note: When the Threat Protection service is running on the Advanced Standalone Appliance, then the GUI and API access is allowed only on the MGMT port.

To enable GUI and API access on the MGMT and LAN1/VIP ports:

1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and select Grid Properties -> Edit.
3. In the Grid Properties editor, select the General tab -> click the Advanced tab (or click Toggle Advanced Mode) and complete the following:
   • Enable GUI/API Access via both MGMT and LAN1/VIP: Select this check box to allow access to the Infoblox GUI and API using both the MGMT and LAN1 ports for standalone appliances and allow both the MGMT and VIP ports for an HA pair. This feature is valid only if you have enabled the MGMT port. For information about enabling the MGMT port, see Appliance Management.
4. Click Save to save the changes.

About Virtual LANs

You can assign VLANs (Virtual Local Area Networks) to the LAN1, LAN2, and VIP (for HA pairs) interfaces so the appliance can provide DNS service to different subnetworks on the same interface. You can also configure VLANs interfaces on supported Network Insight appliances and use them exclusively for discovery purposes. VLANs are independent logical networks that are mutually isolated on the interface so that IP packets can pass between them through one or more switches or routers. You can assign VLANs to provide segmentation services to address issues such as scalability, security, and network management. For example, you can partition your network into segments such as DHCP address allocation, DNS service, guest network, and DMZ (demilitarized zone) to achieve a higher level of security and to increase performance by limiting broadcast domains. You can also add quality of service schemes to optimize your network traffic on the VLAN trunk links by configuring the DSCP (Differentiated Services Code Point) value for the corresponding physical and virtual interfaces. For information about DSCP, see bookmark901 bookmark901.

Note: When you configure VLANs on the following Network Insight appliances: ND-1400, ND-1405, ND-2200, ND-2205, ND-4000, ND-V1400 ND-V1405, ND-V2200, and ND-V2205, the VLAN interfaces are used exclusively for discovery. You cannot bind other services on these VLAN interfaces of the supported Network Insight appliances. For more information about Network Insight, see About Network Insight.

VLAN Tagging

When your VLANs span across multiple networks, VLAN tagging is required. This enables the NIOS appliance to connect to different networks using the same port. VLAN tagging involves adding a VLAN tag or ID to the header of an IP packet so the appliance can identify the VLAN to which the packet belongs. In addition, switches use the VLAN tag to determine the port to which it should send a broadcast packet. The appliance uses the IEEE 802.1Q networking standard to support VLANs and VLAN tagging. On the appliance, you can configure VLANs as tagged networks by adding VLAN tags to them. You can create up to 10 IPv4 and IPv6 addresses per interface and configure a VLAN ID from one to 4094. You can also configure an address, gateway, and a netmask for VLAN. Any IPv4 or IPv6 address with a VLAN ID is considered as a tagged
network. For HA pairs, the appliance supports only one VLAN interface for VRRP over an IPv4 or IPv6. It supports one untagged IPv4 and IPv6 address for each interface and considers this as the primary IP address for the network. For an HA pair, if you have multiple VLANs assigned to a VIP interface, then a network failure in any one of the VLAN interface does not trigger a failover of the active member.

Untagged networks are those without VLAN tags assigned to them. When you set up a VLAN as either a tagged or untagged network, ensure that you properly configure the corresponding switch for the VLAN to function properly.

Note: A tagged VLAN interface receives only those packets that belongs to the tagged network, but an untagged VLAN interface receives all the packets belonging to the tagged and untagged networks of the interface.

VLANs and VLAN tagging are supported on both IPv4 and IPv6 transports. This feature is currently supported on the following Infoblox appliances: Trinzic 1410, 1415, 1420, 1425, 2210, 2215, 2220, 2225, Infoblox-4010, Infoblox-4030-Rev1, Infoblox-4030-Rev2, Infoblox-4030-10G, PT-1400, PT-1405, PT-2200, PT-2205, PT-4000, PT-4000-10GE, TE-1410, TE-1420, TE-1415, and TE-1425. VLAN tagging is not supported on TE-100, TE-810, TE-815, TE-820, and TE-825. For more information about VLAN support for an Infoblox-4030 appliance, refer to the DNS Cache Acceleration Application Guide. For information about these appliances, refer to the respective installation guides on the Infoblox Support web site at http://www.infoblox.com/support.

Currently, only the DNS service can listen on specific VLAN interfaces. The DHCP service listens only on the primary VLAN interface (tagged or untagged). You can also specify VLANs as the source port for sending DNS queries and notify messages. For information about how to configure these, see Specifying Port Settings for DNS.

Additional VLAN support is available exclusively for discovery on the following Network Insight appliances: ND-1400, ND-1405, ND-2200, ND-2205, ND-4000, ND-V1400, ND-V1405, ND-V2200, and ND-V2205. Binding other services on the VLAN interfaces of the Network Insight appliances is not supported.

Note: When you join an appliance that supports VLANs to a Grid that does not support VLANs or revert the appliance to a NIOS version that does not support VLANs, the appliance will become unreachable after joining the Grid or being reverted. You must remove VLAN tagging from the corresponding switch in order to reach the downgraded appliance.

Consider the following guidelines when tagging VLANs on the LAN1 and LAN2 ports:

- You can assign VLAN addresses to an interface and add VLAN tags to them. However, you must designate one of the tagged VLANs as a primary address.
- If the primary IPv4 address is tagged with a VLAN ID, all other addresses on the same interface must be tagged with a VLAN ID as well. You can use the same VLAN ID to tag multiple IPv4 and IPv6 addresses on the same interface. You cannot use the same VLAN ID to tag multiple IPv4 and IPv6 addresses on the same interface.
- You can assign one untagged IPv4 and one untagged IPv6 address to the same interface. These addresses are designated as the primary address for the interface.
- For IPv6, you must have a primary IPv6 address (either tagged or untagged) before you can add other tagged IPv6 addresses on the same interface.
- If you have multiple VLANs assigned to the LAN1 interface and the primary VLAN is untagged, DHCP listens on all VLAN interfaces and thus DHCP lease requests will succeed for the additional VLANs assigned to the LAN1 interface, but the request will actually be handled by the primary untagged VLAN interface.
- You can set up the system to define only tagged networks:
  - When the VLAN tag is not set, the appliance considers the network as an untagged network.
  - You can specify a single untagged IPv4 and IPv6 network per interface.
  - The primary network can be tagged or untagged but you must tag the additional VLANs.

Configuring VLANs

When you first set up a NIOS appliance, you can assign VLANs through the Grid Setup Wizard. For more information, see Using the Setup Wizard. After the initial setup, you can assign VLANs to the LAN1 or LAN2 ports in the Required Ports and Addresses table, as described in bookmark9 08.

On a Grid member, you can assign up to 10 VLANs for each protocol (IPv4 or IPv6) on the LAN1 and LAN2 ports. You can assign up to 10 IPv4 VLAN addresses and 10 IPv6 VLAN addresses for each interface. You can configure only IPv4 VLAN addresses for an IPv4 Grid member and only IPv6 VLAN addresses for an IPv6 Grid member, but for a dual mode Grid member you can configure both IPv4 and IPv6 VLAN addresses. To assign additional VLANs to the LAN1 or LAN2 port, complete the following:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.
2. Select the Network -> Basic tab in the Grid Member Properties editor.
3. In the Additional Ports and Addresses table, click the Add icon and select either MGMT (IPv4), MGMT (IPv6), LAN2 (IPv4), LAN2 (IPv6), Additional Address (loopback) (IPv4), Additional Address (loopback) (IPv6), LAN1 (VMLAN)(IPv4), LAN1 (VMLAN)(IPv6), LAN2 (VMLAN)(IPv4) or LAN2 (VMLAN)(IPv6) from the drop-down list. You can add up to 10 IPv4 and 10 IPv6 VLANs for each interface. Note that you can configure only IPv4 VLAN addresses for an IPv4 Grid member and only IPv6 VLAN addresses for an IPv6 Grid member, but for a dual mode Grid member you can configure both IPv4 and IPv6 VLAN addresses.
   - MGMT (IPv4): Select this to configure IPv4 address for MGMT port. Note that the Infoblox-4030 appliance supports a /32 configuration for IPv4 on MGMT and supports multi-interface only when both LAN1 and MGMT are on the same subnet.
   - MGMT (IPv6): Select this to configure IPv6 address for MGMT port. Note that the Infoblox-4030 appliance supports a /128 prefix configuration for IPv6 on MGMT and supports multi-interface only when both LAN1 and MGMT are on the same subnet.
   - LAN2 (IPv4): Select this to configure IPv4 address for the LAN2 port for DHCP or DNS. Note that Infoblox-4030 appliance supports a /32 configuration for IPv4 on LAN2 and supports multi-interface only when both LAN1 and LAN2 are on the same subnet. This is not applicable to Trinzic 100 appliance.
   - LAN2 (IPv6): Select this to configure IPv6 address for the LAN2 port for DHCP or DNS. Note that Infoblox-4030 appliance supports a /128 prefix configuration for IPv6 on LAN2 and supports multi-interface only when both LAN1 and LAN2 are on the same subnet. This is not applicable to Trinzic 100 appliance.
supports a /128 prefix configuration for IPv6 on LAN2 and supports multi-interface only when both LAN1 and LAN2 are on the same subnet. This is not applicable to Trinzic 100 appliance.

- **Additional Address (loopback) (IPv4):** Select this to add a non-anycast IPv4 address to the loopback interface. Note that you can configure this for IPv4 and dual mode Grid member.
- **Additional Address (loopback) (IPv6):** Select this to add a non-anycast IPv6 address to the loopback interface. Note that you can configure this for IPv6 and dual mode Grid member.

- **LAN1 (VLAN) (IPv4):** Select this to add a VLAN to the LAN1 interface. You can add up to 10 IPv4 VLAN addresses. Note that you can configure this for IPv4 and dual mode Grid member. This is supported on Trinzic 2210, 2215, 2220, 2225, Infoblox-1410, Infoblox-4010, Infoblox-4030-Rev1, Infoblox-4030-Rev2, Infoblox-4030-10G, PT-1400, PT-1405, PT-2200, PT-2205, PT-4000, and PT-4000-10GE appliances. VLAN tagging is not supported on TE-100, TE-810, TE-815, TE-820, TE-825, and vNIOs virtual appliances.
- **LAN1 (VLAN) (IPv6):** Select this to add a VLAN to the LAN1 interface. You can add up to 10 IPv4 and 10 IPv6 VLAN addresses. Note that you can configure this for IPv6 and dual mode Grid member. This is supported on Trinzic 2210, 2215, 2220, 2225, Infoblox-1410, Infoblox-4010, Infoblox-4030-Rev1, Infoblox-4030-Rev2, Infoblox-4030-10G, PT-1400, PT-1405, PT-2200, PT-2205, PT-4000, and PT-4000-10GE appliances.
- **LAN2 (VLAN) (IPv4):** Select this to add a VLAN to the LAN2 interface. You can add up to 10 IPv4 VLAN addresses. Note that you can configure this for IPv4 and dual mode Grid member. This is supported on Trinzic 2210, 2215, 2220, 2225, Infoblox-1410, Infoblox-4010, Infoblox-4030-Rev1, Infoblox-4030-Rev2, Infoblox-4030-10G, PT-1400, PT-1405, PT-2200, PT-2205, PT-4000, and PT-4000-10GE appliances.
- **LAN2 (VLAN) (IPv6):** Select this to add a VLAN to the LAN2 interface. You can add up to 10 IPv6 VLAN addresses. Note that you can configure this for IPv6 and dual mode Grid member. This is supported on Trinzic 2210, 2215, 2220, 2225, Infoblox-1410, Infoblox-4010, Infoblox-4030-Rev1, Infoblox-4030-Rev2, Infoblox-4030-10G, PT-1400, PT-1405, PT-2200, PT-2205, PT-4000, and PT-4000-10GE appliances.

4. Enter the following:

- **Interface:** Displays the name of the VLAN interface. This can be LAN1 (VLAN)(IPv4), LAN1 (VLAN)(IPv6), LAN2 (VLAN)(IPv4) or LAN2 (VLAN)(IPv6) depending on your selection. You cannot modify this.
- **Address:** Type the IP address for the VLAN port.
- **Subnet Mask (IPv4) or Prefix Length (IPv6):** For IPv4 address, specify an appropriate subnet mask and for IPv6 address, specify the prefix length. The prefix length ranges from 2 to 127, with common-sense values ranging from /48 to /127 due to the larger number of bits in the IPv6 address.
- **Gateway:** Type the IPv4 or IPv6 default gateway address for the VLAN port depending on the type of interface. For IPv6 interface, you can also type Automatic to enable the appliance to acquire the IPv6 address of the default gateway and the link MTU from router advertisements. You can now define a link-local address as the default IPv6 gateway and isolate the LAN segment so the local router can provide global addressing and access to the network and Internet. This is supported for both LAN1 and LAN2 interfaces as well as LAN1 and LAN2 in the failover mode.
- **VLAN Tag:** Enter the VLAN tag or ID. You can enter a number from 1 to 4094. Ensure that you configure the corresponding switch accordingly. For information about VLANs, see bookmark899.
- **Port Settings:** For IPv4 only. From the drop-down list, choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose Full for concurrent bidirectional data transmission or Half for data transmission in one direction at a time. Select Automatic to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOs appliances.
- **DSCP Value:** Displays the Grid DSCP value, if configured. To modify, click Override and enter the DSCP value. You can enter a value from 0 to 63. For information about DSCP, see bookmark901 bookmark901.

5. Save the configuration and click Restart if it appears at the top of the screen.

### Implementing Quality of Service Using DSCP

You can implement DiffServ (Differentiated Services) on the appliance by configuring the DSCP (Differentiated Services Code Point) value. DiffServ is a scalable and class-based mechanism that provides relative priorities to the type of services on your network. It can provide low latency for critical network traffic while providing simple best-effort service for non-critical services. The Infoblox DSCP implementation fully conforms to RFC 2475. For more information about DiffServ, refer to RFC 2475, An Architecture for Differentiated Services.

In IPv4 and IPv6 headers, DiffServ uses the DS (Differentiated Services) field for packet classification purposes. The DS field defines the layout of the ToS (Type of Services) octet in IPv4 and the Traffic Class octet in IPv6. The first six bits of the DS field are used as the DSCP value, which determines the PHBs (per-hop behaviors) on DiffServ compliant nodes and enables priorities of services to be assigned to network traffic. For more information about the DS field, refer to RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. When you configure the DSCP value for DiffServ, the appliance sets priorities for all outgoing IP traffic. It implements QoS (quality of service) rules so you can effectively classify and manage your critical network traffic. To ensure that core network services, such as DNS services, continue to operate in the event of network traffic congestion, you can set the DSCP value for the entire Grid and override it at the member level. Note that on an appliance, all outgoing IP traffic on all interfaces uses the same DSCP value.

DSCP is supported on both IPv4 and IPv6 transports and the DSCP value for both IPv4 and IPv6 transports must be the same. This feature is currently supported on the following Infoblox appliances: Trinzic 2210, 2215, 2220, 2225, Infoblox-4010, Infoblox-4030, Infoblox-4030-10GE, PT-1400, PT-1405, PT-2200, PT-2205, PT-4000, PT-4000-10GE, TE-1410, TE-1420, TE-1415, and TE-1425. For information about these appliances, refer to the respective installation guides on the Infoblox Support web site at [http://www.infoblox.com/support](http://www.infoblox.com/support).

**Note:** You can set the DSCP value of the primary LAN using the set network CLI command. For information about the CLI command, refer to the Infoblox CLI Guide. DSCP values for all other interfaces and VLANs must be set through Grid Manager.
Configuring the DSCP Value

The DSCP value is set to zero (lowest priority) by default. You can change this value for the Grid and override the value at the member level. When you configure the DSCP value at the Grid or member level, all outgoing IP traffic on all interfaces uses the same value. Valid DSCP values are from 0 to 63. You can also set the DSCP value using the Infoblox CLI. For more information, refer to the Infoblox CLI Guide. To configure the DSCP value for the Grid:

1. From the Grid tab -> Grid Manager tab, click Grid Properties -> Edit from the toolbar.
2. In the General -> Advanced tab of the Grid Properties editor, complete the following:
   - DSCP Value: Enter a value from 0 to 63. The default is 0 and it represents the lowest priority.
3. Save the configuration.

To override the DSCP value for a member:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.
2. In the Network -> Basic tab of the Grid Member Properties editor, complete the following:
   - DSCP Value: Click Override, and then enter a value from 0 to 63. The default is 0 and it represents the lowest priority.
3. Save the configuration.

You can override the Grid and member DSCP value at the interface level. For more information, see the following:

- For the LAN1 port, see bookmark908
- For the LAN2 port, see Configuring the LAN2 Port.
- For the MGMT port, see Using the MGMT Port.

Ethernet Port Usage

This section provides tables that detail the port usage and source and destination ports for different services, depending on your Grid configuration. bookmark904 displays the type of traffic per port for both Grid and independent deployments. For a more detailed list of the different types of traffic, see bookmark906.

Table 8.3 Appliance Roles and Configuration, Communication Types, and Port Usage

<table>
<thead>
<tr>
<th>Appliance Role</th>
<th>HA Pair</th>
<th>HA Status</th>
<th>MGMT Port</th>
<th>Database Synchronization</th>
<th>Core Network Services</th>
<th>Management Services</th>
<th>GUI Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA Grid Master</td>
<td>Yes</td>
<td>Active</td>
<td>Disabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>LAN1</td>
<td>VIP on HA</td>
</tr>
<tr>
<td>HA Grid Master</td>
<td>Yes</td>
<td>Passive</td>
<td>Disabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Master</td>
<td>No</td>
<td>–</td>
<td>Disabled</td>
<td>LAN1</td>
<td>LAN1</td>
<td>LAN1</td>
<td>–</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Yes</td>
<td>Active</td>
<td>Disabled</td>
<td>LAN1</td>
<td>VIP on HA</td>
<td>LAN1</td>
<td>–</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Yes</td>
<td>Passive</td>
<td>Disabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Member</td>
<td>No</td>
<td>–</td>
<td>Disabled</td>
<td>LAN1</td>
<td>LAN1</td>
<td>LAN1</td>
<td>–</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Yes</td>
<td>Active</td>
<td>Disabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>LAN1</td>
<td>VIP on HA</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Yes</td>
<td>Passive</td>
<td>Disabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1</td>
<td>–</td>
</tr>
<tr>
<td>Single Independent</td>
<td>No</td>
<td>–</td>
<td>Disabled</td>
<td>LAN1</td>
<td>LAN1</td>
<td>LAN1</td>
<td>–</td>
</tr>
<tr>
<td>HA Grid Master</td>
<td>Yes</td>
<td>Active</td>
<td>Enabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
<tr>
<td>HA Grid Master</td>
<td>Yes</td>
<td>Passive</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Master</td>
<td>No</td>
<td>–</td>
<td>Enabled</td>
<td>LAN1</td>
<td>LAN1 or MGMT</td>
<td>MGMT</td>
<td>MGMT and LAN1/VIP</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Yes</td>
<td>Active</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>VIP on HA</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Yes</td>
<td>Passive</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Member</td>
<td>No</td>
<td>–</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>LAN1 or MGMT</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Yes</td>
<td>Active</td>
<td>Enabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Yes</td>
<td>Passive</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Single Independent</td>
<td>No</td>
<td>–</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>MGMT</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Reporting Member</td>
<td>No</td>
<td>–</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>LAN1 or MGMT</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
</tbody>
</table>

Table 8.4 Appliance Roles and Configuration, Communication Types, and Port Usage for Appliances with LAN2 Ports
<table>
<thead>
<tr>
<th>Appliance Role</th>
<th>HA Status</th>
<th>MGMT Po rt</th>
<th>LAN2 P ort</th>
<th>Database Synchronizatio n</th>
<th>Core Network Services</th>
<th>Management Service s</th>
<th>GUI Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA Grid Master</td>
<td>Active</td>
<td>Disabled</td>
<td>Enabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>LAN1 or LAN2</td>
<td>VIP on HA</td>
</tr>
<tr>
<td></td>
<td>Passive</td>
<td>Disabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1 or LAN2</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Master</td>
<td>–</td>
<td>Disabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>LAN1 and/or LAN2</td>
<td>LAN1 or LAN2</td>
<td>LAN1</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Active</td>
<td>Disabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>VIP on HA</td>
<td>LAN1 or LAN2</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Passive</td>
<td>Disabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1 or LAN2</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Member</td>
<td>–</td>
<td>Disabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>LAN1 and/or LAN2</td>
<td>LAN1 or LAN2</td>
<td>–</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Active</td>
<td>Disabled</td>
<td>Enabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>LAN1 or LAN2</td>
<td>VIP on HA</td>
</tr>
<tr>
<td></td>
<td>Passive</td>
<td>Disabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>LAN1 or LAN2</td>
<td>–</td>
</tr>
<tr>
<td>Single Independent</td>
<td>–</td>
<td>Disabled</td>
<td>–</td>
<td>LAN1 and/or LAN2</td>
<td>LAN1 or LAN2</td>
<td>LAN1</td>
<td></td>
</tr>
<tr>
<td>HA Grid Master</td>
<td>Active</td>
<td>Enabled</td>
<td>Enabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
<tr>
<td></td>
<td>Passive</td>
<td>Enabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Master</td>
<td>–</td>
<td>Enabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>LAN1, LAN2 and/or MGMT</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>Active</td>
<td>Enabled</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>VIP on HA</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Passive</td>
<td>Enabled</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Single Grid Member</td>
<td>–</td>
<td>Enabled</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>LAN1, LAN2 and/or MGMT</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>Active</td>
<td>Enabled</td>
<td>Enabled</td>
<td>VIP on HA</td>
<td>VIP on HA</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
<tr>
<td></td>
<td>Passive</td>
<td>Enabled</td>
<td>Enabled</td>
<td>LAN1</td>
<td>–</td>
<td>MGMT</td>
<td>–</td>
</tr>
<tr>
<td>Single Independent</td>
<td>–</td>
<td>Enabled</td>
<td>–</td>
<td>LAN1, LAN2 and/or MGMT</td>
<td>MGMT</td>
<td>MGMT</td>
<td></td>
</tr>
<tr>
<td>Reporting Member</td>
<td>–</td>
<td>Enabled</td>
<td>Enabled</td>
<td>LAN1 or MGMT</td>
<td>LAN1, LAN2 and/or MGMT</td>
<td>MGMT</td>
<td>MGMT</td>
</tr>
</tbody>
</table>

To see the service port numbers and the source and destination locations for traffic that can go to and from a NIOS appliance, see bookmark906. This information is particularly useful for firewall administrators so that they can set policies to allow traffic to pass through the firewall as required.

**Note:** The colors in both tables represent a particular type of traffic and correlate with each other.

**Table 8.5 Sources and Destinations for Services**

<table>
<thead>
<tr>
<th>Service</th>
<th>SRC IP</th>
<th>DST IP</th>
<th>Proto</th>
<th>SRC Port</th>
<th>DST Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Exchange (Member Connection)</td>
<td>LAN1 or MGMT on all Grid members (including Grid Master and Grid Master Candidate)</td>
<td>VIP on HA Grid Master, or LAN1 on single Grid Master Candidate</td>
<td>17 UDP</td>
<td>2114</td>
<td>2114</td>
<td>Initial key exchange for establishing VPN tunnels Required for Grid</td>
</tr>
<tr>
<td></td>
<td>VIP on HA Grid Master Candidate, or LAN1 on single Grid Master Candidate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key Exchange (Grid Master Candidate Promotion)</td>
<td>VIP on HA Grid Master, or LAN1 on single Grid Master Candidate</td>
<td>appliance</td>
<td>17 UDP</td>
<td>2114</td>
<td>2114</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VIP on HA Grid Master Candidate or LAN1 on Single Grid Master Candidate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounting</td>
<td>LAN1 or MGMT on Grid member</td>
<td>VIP on HA Grid Master, or LAN1 on single Grid Master Candidate</td>
<td>17 UDP</td>
<td>1194 or 5002, or 1024 -&gt; 63999</td>
<td>1194 or 5002, or 1024 -&gt; 63999</td>
<td>Default VPN port 1194 for Grids with new DNSone 3.2 installations and 5002 for Grids upgraded to DNSone 3.2; the port number is configurable Required for Grid</td>
</tr>
<tr>
<td>Network Insight VPN</td>
<td>LAN1 or LAN2 on Probes</td>
<td>LAN1 or LAN2 on Consolidator</td>
<td>UDP</td>
<td>1194</td>
<td>1194</td>
<td>All default VPN tunnels for Network Insight</td>
</tr>
<tr>
<td>Service</td>
<td>Description</td>
<td>Protocol(s)</td>
<td>Ports</td>
<td>Purpose / Notes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>LAN1 or LAN2 on Probes</td>
<td>UDP</td>
<td>161</td>
<td>SNMP (Needed for full discovery of some older Check Point models)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>LAN1 or LAN2 on Probes</td>
<td>UDP</td>
<td>260</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>LAN1 or LAN2 on Probes</td>
<td>ICMP</td>
<td>n/a</td>
<td>Ping Sweep</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>LAN1 or LAN2 on Probes</td>
<td>UDP, TCP</td>
<td>53</td>
<td>DNS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>LAN1 or LAN2 on Probes</td>
<td>ICMP</td>
<td></td>
<td>Path Collection. For IPv4 addresses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>LAN1 or LAN2 on Probes</td>
<td>UDP</td>
<td>33434+1 per probe packet</td>
<td>Path Collection. Standard traceroute, for IPv6 addresses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>LAN1 or LAN2 on Probes</td>
<td>ICMP, UDP, TCP</td>
<td></td>
<td>Port scan - all configured by us</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>LAN1 or LAN2 on Probes</td>
<td>UDP</td>
<td>137</td>
<td>NetBIOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>LAN1 or LAN2 on Probes</td>
<td>UDP</td>
<td>40125</td>
<td>NMAP, UDP Ping, and credential checking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>LAN1 or LAN2 on Probes</td>
<td>TCP</td>
<td>23</td>
<td>Telnet can be used based on Network Insight configuration for Network Discovery.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>LAN1 or LAN2 on Probes</td>
<td>TCP</td>
<td>22</td>
<td>SSH can be used based on Network Insight configuration for Network Discovery.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>Client</td>
<td>LAN1, LAN2, VIP, or broadcast on NIOS appliance</td>
<td>17 UDP 68 67</td>
<td>Required for IPv4 DHCP service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>LAN1, LAN2 or VIP on NIOS appliance</td>
<td>Client</td>
<td>17 UDP 67 68</td>
<td>Required for IPv4 DHCP service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>Client</td>
<td>LAN1, LAN2, VIP, or broadcast on NIOS appliance</td>
<td>17 UDP 546 547</td>
<td>Required for IPv6 DHCP service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>LAN1, LAN2 or VIP on NIOS appliance</td>
<td>Client</td>
<td>17 UDP 547 546</td>
<td>Required for IPv6 DHCP service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Failover</td>
<td>LAN1, LAN2 or VIP on Infoblox DHCP failover peer</td>
<td>LAN1, LAN2 of VIP on Infoblox DHCP failover peer</td>
<td>6 TCP 1024 65535 519, or 647</td>
<td>Required for DHCP failover</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Failover</td>
<td>VIP on HA Grid Master or LAN1 or LAN2 on single master</td>
<td>LAN1, LAN2 or VIP on Grid member in a DHCP failover pair</td>
<td>6 TCP 1024 -&gt; 65535 7911</td>
<td>Informs functioning Grid member in a DHCP failover pair that its partner is down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DDNS Updates</td>
<td>LAN1, LAN2, or VIP</td>
<td>LAN1, LAN2, or VIP</td>
<td>17 UDP 1024 65535 53</td>
<td>Required for DHCP to send DNS dynamic updates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Transfers</td>
<td>LAN1, LAN2, VIP, or MGMT, or client</td>
<td>LAN1, LAN2, VIP, or MGMT</td>
<td>6 TCP 53, or 1024 -&gt; 65535 53</td>
<td>For DNS zone transfers, large client queries, and for Grid members to communicate with external name servers</td>
<td>Required for DNS</td>
<td></td>
</tr>
<tr>
<td>DNS Queries</td>
<td>Client</td>
<td>LAN1, LAN2, VIP, or broadcast on NIOS appliance</td>
<td>17 UDP 53, or 1024 65535 53</td>
<td>For DNS queries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Queries</td>
<td>Client</td>
<td>LAN1, LAN2, VIP, or broadcast on NIOS appliance</td>
<td>6 TCP 53, or 1024 65535 53</td>
<td>For DNS queries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>NTP client</td>
<td>LAN1, LAN2, VIP, or MGMT</td>
<td>17 UDP 1024 -&gt; 65535 123</td>
<td>Required if the NIOS appliance is an NTP server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Type</td>
<td>Source IP Address</td>
<td>Destination IP Address</td>
<td>Port range</td>
<td>Protocol</td>
<td>Source Port</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>--------------------------------------------</td>
<td>-------------------------</td>
<td>------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>NTP</td>
<td>NTP client</td>
<td>LAN1, LAN2, VIP, or MGMT</td>
<td></td>
<td>17 UDP</td>
<td>UDP</td>
<td>1024 -&gt; 65535</td>
</tr>
<tr>
<td>RADIUS Authentication</td>
<td>NAS (network access server)</td>
<td>LAN1 or VIP</td>
<td></td>
<td>17 UDP</td>
<td>UDP</td>
<td>1024 – 65535</td>
</tr>
<tr>
<td>RADIUS Accounting</td>
<td>NAS (network access server)</td>
<td>LAN1 or VIP</td>
<td></td>
<td>17 UDP</td>
<td>UDP</td>
<td>1024 – 65535</td>
</tr>
<tr>
<td>RADIUS Proxy</td>
<td>LAN1 or VIP</td>
<td>RADIUS home server</td>
<td></td>
<td>17 UDP</td>
<td>UDP</td>
<td>1814</td>
</tr>
<tr>
<td>ICMP Dst Port Unreachable</td>
<td>VIP, LAN1, LAN2, or MGMT, or UNIX-based client</td>
<td>LAN1, LAN2, or UNIX-based client</td>
<td></td>
<td>1 ICMP Type 3</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>ICMP Echo Reply</td>
<td>VIP, LAN1, LAN2, or MGMT, or client</td>
<td>VIP, LAN1, LAN2, or MGMT, or client</td>
<td></td>
<td>1 ICMP Type 0</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>ICMP Echo Request</td>
<td>VIP, LAN1, LAN2, or MGMT, or client</td>
<td>VIP, LAN1, LAN2, or MGMT, or client</td>
<td></td>
<td>1 ICMP Type 8</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>ICMP TTL Exceeded</td>
<td>Gateway device (router or firewall)</td>
<td>Windows client</td>
<td></td>
<td>1 ICMP Type 11</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>NTP</td>
<td>LAN1 on active node of Grid Master or LAN1 of independent appliance</td>
<td>NTP server</td>
<td></td>
<td>17 UDP</td>
<td>UDP</td>
<td>1024 -&gt; 65535</td>
</tr>
<tr>
<td>SMTP</td>
<td>LAN1, LAN2, or VIP</td>
<td>Mail server</td>
<td></td>
<td>6 TCP</td>
<td>TCP</td>
<td>1024 65535</td>
</tr>
<tr>
<td>SNMP</td>
<td>NMS (network management system) server</td>
<td>VIP, LAN1, LAN2, or MGMT</td>
<td></td>
<td>17 UDP</td>
<td>UDP</td>
<td>1024 65535</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>MGMT or LAN1 on Grid Master or HA pair, or LAN1 on independent appliance</td>
<td>NMS server</td>
<td></td>
<td>17 UDP</td>
<td>UDP</td>
<td>1024 -&gt; 65535</td>
</tr>
<tr>
<td>Service</td>
<td>Type</td>
<td>Description</td>
<td>Protocol</td>
<td>Port Range</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>SSHv2</td>
<td>Client</td>
<td>LAN1, LAN2, VIP, or MGMT on NIOS appliance</td>
<td>TCP</td>
<td>1024 -&gt; 65535</td>
<td>22 Administrators can make an SSHv2 connection to the LAN1, LAN2, VIP, or MGMT port</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Optional for management</td>
<td></td>
</tr>
<tr>
<td>Syslog</td>
<td></td>
<td>syslog server</td>
<td>UDP</td>
<td>1024</td>
<td>514 Required for remote syslog logging</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LAN1, LAN2, or MGMT of NIOS appliance</td>
<td></td>
<td>65535</td>
<td>Optional for management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VIP, LAN1, LAN2, or MGMT, or client</td>
<td>UDP</td>
<td>1024</td>
<td>NIOS appliance responds with ICMP type code 3 (port unreachable)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multicast address 224.0.0.18</td>
<td></td>
<td></td>
<td>For periodic announcements of the availability of the HA node that is linked to the VIP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VRRP</td>
<td></td>
<td>1024</td>
<td>65535 For contacting a TFTP server during database and configuration backup and restore</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Traceroute</td>
<td></td>
<td>1024</td>
<td>65535 For contacting a TFTP server during database and configuration backup and restore</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional for management</td>
<td></td>
<td>17</td>
<td>For remote syslog logging</td>
<td></td>
</tr>
<tr>
<td>VRRP</td>
<td></td>
<td>HA IP on the active node of HA pair</td>
<td>UDP</td>
<td>1024</td>
<td>65535 For periodic announcements of the availability of the HA node that is linked to the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multicast address 224.0.0.18</td>
<td></td>
<td>65535</td>
<td>VIP. The nodes in the HA pair must be in the same subnet.</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>Management</td>
<td>VIP, LAN1, or MGMT</td>
<td>TCP</td>
<td>1024 -&gt; 65535</td>
<td>80 Required if the HTTP-redirect option is set on the Grid properties security page</td>
<td></td>
</tr>
<tr>
<td>HTTPS/SSL</td>
<td>Management</td>
<td>VIP, LAN1, or MGMT</td>
<td>TCP</td>
<td>1024</td>
<td>65535 Required for administration through the GUI</td>
<td></td>
</tr>
<tr>
<td>Reporting</td>
<td>Reporting</td>
<td>LAN1, LAN2, or MGMT on the indexer</td>
<td>TCP</td>
<td>1024 -&gt; 65535</td>
<td>9997 Required for the reporting service. Communication is single directional from</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Forwarders</td>
<td></td>
<td></td>
<td></td>
<td>forwards to the indexer. For example, a forwarder detects events and forwards them to</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>the indexer.</td>
<td></td>
</tr>
<tr>
<td>Reporting - Peer</td>
<td>Reporting</td>
<td>LAN1, LAN2, MGMT on each reporting member</td>
<td>TCP</td>
<td>1024</td>
<td>7887 Splunk cluster peer replication (traffic among reporting members)</td>
<td></td>
</tr>
<tr>
<td>Replication</td>
<td>All Reporting</td>
<td></td>
<td></td>
<td>65535</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed</td>
<td>All Reporting</td>
<td>LAN1, LAN2, MGMT on each reporting member</td>
<td>TCP</td>
<td>1024</td>
<td>7089 Distributed searches from Search Head to Reporting Members</td>
<td></td>
</tr>
<tr>
<td>Search</td>
<td>Members</td>
<td></td>
<td></td>
<td>65535</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting</td>
<td>All Reporting</td>
<td>LAN1, LAN2, MGMT on each reporting member</td>
<td>TCP</td>
<td>1024</td>
<td>8089 Grid Master to reporting members</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Members</td>
<td></td>
<td></td>
<td>65535</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting</td>
<td>All Reporting</td>
<td>LAN1, LAN2, MGMT on each reporting member</td>
<td>TCP – IPv4</td>
<td>1024 - 65535</td>
<td>8000 Grid Master to reporting members</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Members</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting</td>
<td>All Reporting</td>
<td>VIP on HA Grid Master or MGMT on single appliance (with threat protection</td>
<td>TCP – IPv6</td>
<td>1024 - 65535</td>
<td>8000 Grid Master to reporting members</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Members</td>
<td>service running)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Protection</td>
<td>VIP on HA Grid</td>
<td>N/A (using FQDN = <a href="https://ts.infoblox.c">https://ts.infoblox.c</a>) HTTPS N/A 443 For threat protection rule updates.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Dynamic Port</td>
<td>Management server</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Insight</td>
<td>Client</td>
<td>N/A (using FQDN = <a href="https://ts.infoblox.co">https://ts.infoblox.co</a>) HTTPS N/A 443 For downloading module set and whitelist updates.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Modifying Ethernet Port Settings

By default, the NIOS appliance automatically negotiates the optimal connection speed and transmission type (full or half duplex) on the physical links between the 10/100Base-T and 10/100/1000Base-T ports on the NIOS appliance and the Ethernet ports on a connecting switch. It is usually unnecessary to change the default auto-negotiation setting; however, you can manually configure connection settings for a port if necessary. Occasionally, for example, even though both the NIOS appliance and the connecting switch support 1000-Mbps (megabits per second) full-duplex connections, they might fail to auto-negotiate that speed and type, and instead connect at lower speeds of either 100 or 10 Mbps using potentially mismatched full- and half-duplex transmissions. If this occurs, first determine if there is a firmware upgrade available for the switch. If so, apply the firmware upgrade and test the connection. If that does not resolve the issue, manually set the ports on the NIOS appliance and on the switch to make 1000-Mbps full-duplex connections.

To change Ethernet port settings:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.
   **Note:** You must enable the MGMT port before modifying its port settings. See Using the MGMT Port.
2. In the Network tab of the Grid Member Properties editor, the Required Ports and Addresses table lists the network settings that were configured. This table lists the network settings of LAN1 (IPv4) interface for an IPv4 member and LAN1 (IPv6) interface for an IPv6 member. For a dual mode Grid member, this table lists the settings for both LAN1 (IPv4) and LAN1 (IPv6) interfaces. Complete the following to modify port settings:
   - **Interface:** Displays the name of the interface. You cannot modify this.
   - **Address:** Click the field and modify the IP address for the LAN1 port, which must be in a different subnet from that of the LAN2 and HA ports.
   - **Subnet Mask (IPv4) or Prefix Length (IPv6):** For IPv4 address, click the field and specify an appropriate subnet mask and for IPv6 address, specify the prefix length.
   - **Gateway:** Click the field and modify the default gateway for the LAN1 port.
   - **VLAN Tag:** Click the field and enter the VLAN tag ID if the port is configured for VLANs. You can enter a number from 1 to 4095.
     For information about VLAN, see bookmark989.
   - **Port Settings:** From the drop-down list, choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose Full for concurrent bidirectional data transmission or Half for data transmission in one direction at a time. Select Automatic to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOS appliances.
   - **DSCP Value:** Displays the Grid DSCP value. To modify, click Override and enter the DSCP value. You can enter a value from 0 to 63. For information about DSCP, see bookmark901 bookmark901.
3. Save the configuration and click Restart if it appears at the top of the screen.

**Note:** The port settings on the connecting switch must be identical to those you set on the NIOS appliance.

Using the LAN2 Port

**Note:** This feature is not supported on vNIOS Grid members for Riverbed.

The LAN2 port is a 10/100/1000Base-T Ethernet connector on the front panel of the TE-810, TE-820, TE-1410, TE-1420, TE-2210, TE-2220, and IB-4010 appliances. By default, the LAN2 port is disabled and the appliance uses the LAN1 port (and HA port when deployed in an HA pair). Before you can enable and configure the LAN2 port on a Grid member, you must first configure the member and join it to the Grid. You must also have read/write permission to the Grid member on which you want to enable the port. When you enable the LAN2 port and SNMP, the appliance sends traps from this port for LAN2 related events.

You can configure the LAN2 port in different ways. You can enable the port redundancy or port failover feature, which groups the LAN1 and LAN2 ports into one logical interface. The LAN1/LAN2 grouping can be activated for both IPv4 and IPv6. Alternatively, you can configure the LAN2 port on a different IP network than LAN1, and enable the LAN2 port to provide DNS and DHCP services. For information about these features, see the following sections:

- For information about the LAN2 failover feature, see bookmark913.
- For information about configuring the LAN2 port, see bookmark916.
- For information about enabling the LAN2 port to provide DHCP services, see bookmark917.
- For information about enabling the LAN2 port to provide DNS services, see bookmark919.

**Note** that you cannot use the LAN2 port to access the GUI and the API, or to connect to the Grid. This can impact the ability of other appliances, such as the Network Automation and PortIQ appliances, to communicate with the Grid Master.

Any IPv6 services enabled for the LAN2 port also require provisioning of an IP address on the LAN2 port.

About Port Redundancy

You can configure the LAN2 or LAN2 (VLAN) port to provide redundancy and additional fault tolerance in your network. Port redundancy is transparently supported for both IPv4 and IPv6. When you enable port redundancy, the LAN1 or LAN1 (VLAN) and LAN2 or LAN2 (VLAN) ports are grouped into one logical interface. They share one IP address and appear as one interface to the network. Then, if a link to one of the ports fails or is disabled, the appliance fails over to the other port, avoiding a service disruption.
You can connect the LAN1 or LAN1 (VLAN) and LAN2 or LAN2 (VLAN) ports to the same switch or to different switches, but they must be on the same VLAN. One port is active and the other port is idle at all times. In case of failure in the LAN1 or LAN1 (VLAN) port, the LAN2 or LAN2 (VLAN) port becomes active and once the LAN1 or LAN1 (VLAN) port is active again, the LAN2 or LAN2 (VLAN) port becomes passive.

**Note:** When configuring port redundancy, the speed of the interfaces is not taken into consideration when selecting the active interface.

The LAN1 or LAN1 (VLAN) and LAN2 or LAN2 (VLAN) ports share the IP address of the LAN1 or LAN1 (VLAN) port; the port that is currently active owns the IP address. When you enable services on the appliance, such as DNS and DHCP, clients send their service requests to the LAN1 or LAN1 (VLAN) port IP address and receive replies from it as well. The port supports the services and features supported on the LAN1 or LAN1 (VLAN) port as listed in Table 8.4 and Table 8.5. You cannot enable the port redundancy feature if the LAN2 or LAN2 (VLAN) port is serving DNS or DHCP.

For example, you can use the MGMT port for Grid communications, as shown in bookmark915, and the LAN1 and LAN2 ports are connected to the same switch. The LAN1 and LAN2 port share the IP address of the LAN1 port, which is 1.1.1.5. In the illustration, LAN1 is the active port.

You can also have the MGMT port disabled and configure LAN1 and LAN2 for port redundancy. You can enable port redundancy on single or HA independent appliances and Grid members. Note that NIC bonding is not supported for OpenStack instances.

**Figure 8.6 Using the LAN2 Failover Feature**

Before you enable port redundancy, ensure that both LAN1 and LAN2 are enabled. To enable port redundancy:

1. From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **Grid_member** check box, and then click the Edit icon.
2. In the **Network -> Basic** tab of the **Grid Member Properties** editor, select the **Enable port redundancy on LAN/LAN2** check box.
3. Save the configuration and click **Restart** if it appears at the top of the screen.

The **Detailed Status** panel displays the status of both the LAN1 and LAN2 ports. In an HA pair, both nodes display the port information when port redundancy is enabled.
### Configuring the LAN2 Port

Before you enable the LAN2 port to provide DHCP and DNS services, you must specify its IP address and other properties. You can configure both IPv4 and IPv6 addresses for the LAN2 port of an IPv4, IPv6 and dual mode (IPv4 and IPv6) Grid member.

To configure the LAN2 port:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.
2. In the Network -> Basic tab of the GridMemberProperties editor, click the Add icon of the Additional Ports and Addresses table and select LAN2(IPV4) or LAN2(IPV6) from the drop-down list. Enter the following:
   - Interface: Displays the name of the interface. You cannot modify this.
   - Address: Type the IP address for the LAN2 port, which must be in a different subnet from that of the LAN1 and HA ports.
   - Subnet Mask (IPv4) or Prefix Length (IPv6): Specify an appropriate subnet mask for IPv4 address and prefix length for IPv6 address.
   - Gateway: Type the default gateway for the LAN2 port.
   - VLAN Tag: Enter the VLAN tag ID if the port is configured for VLANs. You can enter a number from 1 to 4095. For information about VLAN, see About Virtual LANs.
   - Port Settings: From the drop-down list, choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose Full for concurrent bidirectional data transmission or Half for data transmission in one direction at a time. Select Automatic to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOS appliances.
   - DSCP Value: Displays the Grid DSCP value. To modify, click Override and then enter the DSCP value. You can enter a value from 0 to 63. For information about DSCP, see Implementing Quality of Service Using DSCP.
   - LAN2 Virtual Router ID (if HA): If the appliance is in an HA pair, enter a VRID number.
3. Save the configuration and click Restart if it appears at the top of the screen.

The Detailed Status panel displays the status of the LAN2 port. In an HA pair, only the active node displays the LAN2 information.

### Enabling DHCP on LAN2

You can configure an appliance to provide DHCP service through the LAN1 port, LAN2 port, or both the LAN1 and LAN2 ports. Note that when you enable both ports, they must be connected to different subnets. You can also start and stop DHCP service for IPv4 or IPv6 on the LAN1 or LAN2 port after you have enabled the service.

After you configure the LAN2 port, you can enable DHCP services on the LAN2 port as follows:

1. From the Data Management tab, select the DHCP tab -> Members tab -> Grid_member check box, and then click the Edit icon.
2. If you are running DHCP for IPv4: In the General -> Basic tab of the Member DHCP Configuration editor, select the IPv4 check box for LAN2 under DHCP Interfaces.
   
   If you are running DHCP for IPv6: In the General -> Basic tab of the Member DHCP Configuration editor, select the IPv6 check box for LAN2 under DHCP Interfaces. (An IPv6 address must also be provisioned for the port.)

   You can run either or both protocols for DHCP depending on your network deployment.
3. Save the configuration and click Restart if it appears at the top of the screen.

### Enabling DNS on LAN2

If you enable DNS on an appliance, it always serves DNS on the LAN1 port. Optionally, you can configure the appliance to provide DNS services through the LAN2 port as well. For example, the appliance can provide DNS services through the LAN1 port for internal clients on a private network, and DNS services through the LAN2 port for external clients on a public network.

After you configure the LAN2 port, you can enable DNS services on the LAN2 port as follows:

1. From the Data Management tab, select the DNS tab -> Members tab -> Grid_member check box, and then click the Edit icon.
2. In the General -> Basic tab of the Member DNS Configuration editor, do the following:
   
   If you are running DNS for IPv4: In the General -> Basic tab of the Member DHCP Configuration editor, select the IPv4 check box for LAN2 under DNS Interfaces.

   If you are running DNS for IPv6: In the General -> Basic tab of the Member DHCP Configuration editor, select the IPv6 check box for LAN2 under DNS Interfaces. (An IPv6 address must also be provisioned for the port.)

   You can run either or both protocols for DNS depending on your network deployment.

   Automatically create glue A and PTR records for LAN2's address: The NIOS appliance can automatically generate A (address) and PTR records for a primary name server whose host name belongs to the name space of the zone. Select this check box to enable the appliance to automatically generate an A and PTR record.

   Automatically create IPv6 glue AAAA and PTR records for LAN2's address: automatically generate AAAA and PTR records for the LAN2 IPv6 address. A glue record is the IP address of a name server held at the domain name registry. They are needed to set a domain's name server to a host name within the domain. Example: to set the name servers of ns1.corpxyz.com and ns2.corpxyz.com, provide the glue records, which are in effect the IP addresses, for ns1.corpxyz.com and ns2.corpxyz.com, within specific DNS record types.

   Without the glue records, DNS requests never resolve to the correct IP address because the domain registry does not associate the IP with the correct records.

3. In the General -> Advanced tab (click Toggle Advanced Mode if necessary), select one of the following from the Send queries from add the Send notify messages and zone transfer request from drop-down lists:
• **VIP**: The appliance uses the IP address of the HA port as the source for queries, notifies, and zone transfer requests.
• **MGMT**: The appliance uses the IP address of the MGMT port as the source for queries, notifies, and zone transfer requests.
• **LAN2**: The appliance uses the IP address of the LAN2 port as the source for queries, notifies, and zone transfer requests.
• **Any**: The appliance chooses which port to use as the source for queries, notifies, and zone transfer requests.

The **Send queries from** drop-down list also includes loopback IP addresses that you configured. You can select a loopback address as the source for queries.

1. Save the configuration and click **Restart** if it appears at the top of the screen.
2. Click **Restart** to restart services.

### Using the MGMT Port

**Note**: This feature is not supported on vNIOS Grid members for Riverbed.

The MGMT (Management) port is a 10/100/1000Base-T Ethernet connector on the front panel of the TE-810, TE-820, TE-1410, TE-1420, TE-2210, TE-2220, and IB-4010 appliances. It allows you to isolate the following types of traffic from other types of traffic on the LAN and HA ports:

- **Appliance Management**
- **Grid Communications**
- **DNS Services**

For information about what types of traffic qualify as appliance management, Grid communications, and DNS services, see Table 8.5.

**Note**: The MGMT port currently does not support DHCP, NAT, or TFTP. IPv6 addressing may be applied to the MGMT port.

Some NIOS appliance deployment scenarios support more than one concurrent use of the MGMT port. The following table depicts MGMT port uses for various appliance configurations.

<table>
<thead>
<tr>
<th>Appliance Configuration</th>
<th>Appliance Management</th>
<th>Grid Communications</th>
<th>DNS Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Independent Appliance</td>
<td>✓</td>
<td>Not Applicable</td>
<td>✓</td>
</tr>
<tr>
<td>Independent HA Pair</td>
<td>✓</td>
<td>Not Applicable</td>
<td></td>
</tr>
<tr>
<td>Grid Master</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grid Master Candidate</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HA Grid Member</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Single Grid Member</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

* Although you manage all Grid members through the Grid Master, if you enable the MGMT port on common Grid members, they can send syslog events, SNMP traps, and e-mail notifications, and receive SSH connections on that port. Infoblox does not support MGMT port usage for some appliance configurations (indicated by the symbol ✶ in Table 8.6) because it cannot provide redundancy through the use of a VIP. A Grid Master that is an HA pair needs the redundancy that a VIP interface on the HA port provides for Grid communications. Similarly, DNS servers in an HA pair need that redundancy to answer DNS queries. Because the MGMT port does not support a VIP and thus cannot provide redundancy, Grid Masters (and potential Grid Masters) do not support Grid communications on the MGMT port.

In addition, NIOS appliances in an HA pair support DNS services on the active node only (indicated by the symbol ✶✶ in Table 8.6). Only the active node can respond to queries that it receives. If a DNS client sends a query to the MGMT port of the node that happens to be the passive node, the query can eventually time out and fail.

The MGMT port is not enabled by default. By default, a NIOS appliance uses the LAN port (and HA port when deployed in an HA pair). You must log in using a superuser account to enable and configure the MGMT port. You can configure both IPv4 address and IPv6 address for the MGMT port of a Grid member. You can enable the MGMT port through the Infoblox GUI, as explained in the following sections.

### Appliance Management

You can restrict administrative access to a NIOS appliance by connecting the MGMT port to a subnet containing only management systems. This approach ensures that only appliances on that subnet can access the Infoblox GUI and receive appliance management communications such as syslog events, SNMP traps, and e-mail notifications from the appliance.
If you are the only administrator, you can connect your management system directly to the MGMT port. If there are several administrators, you can define a small subnet—such as 10.1.1.0/29, which provides six host IP addresses (10.1.1.1–10.1.1.6) plus the network address 10.1.1.0 and the broadcast address 10.1.1.7—and connect to the NIOS appliance through a dedicated switch (which is not connected to the rest of the network). Figure 8.7 shows how an independent appliance separates appliance management traffic from network protocol services. Note that the LAN port is on a different subnet from the MGMT port.

**Figure 8.7 Appliance Management from One or More Management Systems**

Similarly, you can restrict management access to a Grid Master to only those appliances connected to the MGMT ports of the active and passive nodes of the Grid Master.

To enable the MGMT port on an independent appliance or Grid Master for appliance management and then cable the MGMT port directly to your management system or to a network forwarding appliance such as a switch or router:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> grid_member check box, and then click the Edit icon.
2. In the Network -> Basic tab of the Grid Member Properties editor, add the MGMT port to the Additional Ports and Addresses table as follows:
3. Click the Add icon and select MGMT (IPv4) to configure an IPv4 address or select MGMT (IPv6) to configure an IPv6 address for the MGMT port. You can configure both IPv4 and IPv6 addresses for the MGMT port. Grid Manager adds a row for the MGMT port. For an HA pair, it adds two rows, one for each node.
4. Enter the following in the row of the MGMT port for a single Grid Master or independent appliance, and in the rows of the two nodes for an HA Grid Master or independent HA pair:
   - **Interface**: Displays the name of the interface. You cannot modify this.
   - **Address**: Type the IP address for the MGMT port, which must be in a different subnet from that of the LAN and HA ports.
   - **Subnet Mask (IPv4) or Prefix Length (IPv6)**: For IPv4 address, specify an appropriate subnet mask for the number of management systems that you want to access the appliance through the MGMT port. For IPv6 address, specify the prefix length.
   - **Gateway**: Type the default gateway for the MGMT port. If you need to define any static routes for traffic originating from the MGMT port—such as SNMP traps, syslog events, and email notifications—destined for remote subnets beyond the immediate subnet, specify the IP address of this gateway in the route.
   - **Port Settings**: Choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose Full for concurrent bidirectional data transmission or Half for data transmission in one direction at a time. Select Automatic to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOS appliances.
4. **DSCP Value**: Displays the Grid DSCP value. To modify, click Override and then enter the DSCP value. You can enter a value from 0 to 63. For information about DSCP, see *Implementing Quality of Service Using DSCP*.

5. In the **Network -> Advanced** tab, make sure that the **Enable VPN on MGMT Port** check box is not selected.

6. Save the configuration and click **Restart** if it appears at the top of the screen.

7. Log out of Grid Manager.

8. Cable the MGMT port to your management system or to a switch or router to which your management system can also connect.

9. If your management system is in a subnet from which it cannot reach the MGMT port, move it to a subnet from which it can.

   The Infoblox Grid Manager GUI is now accessible through the MGMT port on the NIOS appliance from your management system.

10. Open an Internet browser window and enter the IP address of the MGMT port as follows: `https://<IP address of MGMT port>`.

11. Log in to Grid Manager.

12. Check the **Detailed Status** panel of the Grid member to make sure the status icons are green.

**Grid Communications**

You can isolate all Grid communications to a dedicated subnet as follows:

- For Grid communications from the Grid Master, which can be an HA pair or a single appliance, the master uses either the VIP interface on the HA port of its active node (HA master) or its LAN port (single master). Neither a single nor HA Grid Master can use its MGMT port for Grid communications. (This restriction applies equally to Master Candidates.)

- Common Grid members connect to the Grid Master through their MGMT port.

This ensures that all database synchronization and Grid maintenance operations are inaccessible from other network elements while the common Grid members provide network protocol services on their LAN ports.

*Figure 8.8* shows how Grid members communicate to the master over a dedicated subnet.

*Figure 8.8 Grid Communications*
Enabling Grid Communications over the MGMT Port for Existing Grid Members

To enable the MGMT port for Grid communications on an existing single or HA Grid member:

1. Log in to the Grid Master with a superuser account.
2. From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **Grid member** check box, and then click the Edit icon.

   **Note:** You must enable the MGMT port before modifying its port settings. See *Using the MGMT Port*.

3. In the **Network** -> **Basic** tab of the **Grid Member Properties** editor, add the MGMT port to the Additional Ports and Addresses table as follows:
4. Click the Add icon and select **MGMT (IPv4)** to configure an IPv4 address or select **MGMT (IPv6)** to configure an IPv6 address for the MGMT port. You can configure both IPv4 address and IPv6 address for the MGMT port.
5. Grid Manager adds a row for the MGMT port. For an HA pair, it adds two rows, one for each node.
6. Enter the following in the row of the MGMT port for a single Grid Master or independent appliance, and in the rows of the two nodes for an HA Grid Master or independent HA pair:
   - **Interface:** Displays the name of the interface. You cannot modify this.
   - **Address:** Type the IP address for the MGMT port, which must be in a different subnet from that of the LAN and HA ports.
   - **Subnet Mask (IPv4) or Prefix Length (IPv6):** For IPv4 address, specify an appropriate subnet mask for the number of management systems that you want to access the appliance through the MGMT port. For IPv6 address, specify the prefix length.
   - **Gateway:** Type the default gateway for the MGMT port. If you need to define any static routes for traffic originating from the MGMT port—such as SNMP traps, syslog events, and email notifications—destined for remote subnets beyond the immediate

---

* Only the active node of an HA member connects to the Grid Master. The passive node communicates just with the active node. If there is an HA failover, the newly promoted active node must first join the Grid before continuing Grid communications with the Grid Master on behalf of the HA member.
subnet, specify the IP address of this gateway in the route.

- **Port Settings**: Choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose **Full** for concurrent bidirectional data transmission or **Half** for data transmission in one direction at a time. Select **Automatic** to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOS appliances.

- **DSCP Value**: Displays the Grid DSCP value. To modify, click **Override** and enter the DSCP value. You can enter a value from 0 to 63. For information about DSCP, see *Implementing Quality of Service Using DSCP*.

6. In the **Network -> Advanced** tab, select the **Enable VPN on MGMT Port** check box.

7. In the **Security** tab, do the following:
   - **Restrict Remote Console and Support Access to MGMT Port**: Select this check box to restrict SSH (Secure Shell) v2 access to the MGMT port only. This restricts Infoblox Technical Support and remote console connections—both of which use SSH v2—to just the MGMT port. For an HA pair, you can make an SSH v2 connection to the MGMT port on both the active and passive nodes. Clear the check box to allow SSH v2 access to both the MGMT and LAN ports. For an HA pair, you can make an SSH v2 connection to the MGMT and LAN ports on both the active and passive nodes.

8. Save the configuration and click **Restart** if it appears at the top of the screen.
   The master communicates the new port settings to the member, which immediately begins using them. The member stops using its LAN port for Grid communications and begins using the MGMT port.

9. To confirm that the member still has Grid connectivity, check that the status icons for that member are green on the **Detailed Status** and **Grid** panels.

**DNS Services**

You can configure a single independent appliance or single Grid member to provide DNS services through the MGMT port in addition to the LAN port. For example, the appliance can provide DNS services through the MGMT port for internal clients on a private network, and DNS services through the LAN port for external clients on a public network.

While providing DNS services on the MGMT port, you can still use that port simultaneously for appliance management. **Figure 8.9** shows a management system communicating with a single independent appliance through its MGMT port while the appliance also provides DNS services on that port to a private network. Additionally, the appliance provides DNS services to an external network through its LAN port.

**Figure 8.9 DNS Services on the LAN and MGMT Ports, and appliance Management on the MGMT Port**

Like a single independent appliance, a single Grid member can also support concurrent DNS traffic on its MGMT and LAN ports. However, because you manage all Grid members through the Grid Master, a Grid member only uses an enabled MGMT port to send SNMP traps, syslog events, and email notifications, and to receive SSH connections.

In addition, the active node of an HA pair can provide DNS services through its MGMT port. To use this feature, you must enable DNS services on the MGMT ports of both nodes in the HA pair and specify the MGMT port IP addresses of both nodes on the DNS client as well, in case there...
is a failover and the passive node becomes active. Note that only the active node can respond to queries that it receives. If a DNS client sends a query to the MGMT port of the node that happens to be the passive node, the query can eventually time out and fail.

To enable DNS services on the MGMT port of an appliance:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.

   **Note:** You must enable the MGMT port before modifying its port settings. See Using the MGMT Port.

2. In the Network -> Basic tab of the Grid Member Properties editor, add the MGMT port to the Additional Ports and Addresses table as follows:

3. Click the Add icon and select MGMT (IPv4) to configure an IPv4 address or select MGMT (IPv6) to configure an IPv6 address for the MGMT port. You can configure both IPv4 and IPv6 address for the MGMT port.

   Grid Manager adds a row for the MGMT port. For an HA pair, it adds two rows, one for each node.

4. Enter the following in the row of the MGMT port for a single Grid Master or independent appliance, and in the rows of the two nodes for an HA Grid Master or independent HA pair:

   - **Interface:** Displays the name of the interface. You cannot modify this.
   - **Address:** Type the IP address for the MGMT port, which must be in a different subnet from that of the LAN and HA ports.
   - **Subnet Mask (IPv4) or Prefix Length (IPv6):** For IPv4 address, specify an appropriate subnet mask for the number of management systems that you want to access the appliance through the MGMT port. For IPv6 address, specify the prefix length.
   - **Gateway:** Type the default gateway for the MGMT port. If you need to define any static routes for traffic originating from the MGMT port—such as SNMP traps, syslog events, and email notifications—destined for remote subnets beyond the immediate subnet, specify the IP address of this gateway in the route.
   - **Port Settings:** Choose the connection speed that you want the port to use. You can also choose the duplex setting. Choose Full for concurrent bidirectional data transmission or Half for data transmission in one direction at a time. Select Automatic to instruct the NIOS appliance to negotiate the optimum port connection type (full or half duplex) and speed with the connecting switch automatically. This is the default setting. You cannot configure port settings for vNIOS appliances.
   - **DSCP Value:** Displays the Grid DSCP value. To modify, click Override and enter the DSCP value. You can enter a value from 0 to 63. For information about DSCP, see Implementing Quality of Service Using DSCP.

5. Click Save & Close to save your settings for the MGMT port.

6. From the Data Management tab, select the DNS tab -> Members tab -> Grid_member check box, and then click the Edit icon.

7. In the General -> Basic tab of the Member DNS Properties editor, do the following:

   - If you are running DNS service for IPv4, select the IPv4 check box for MGMT under DNS Interfaces.
   - If you are running DNS service for IPv6, select the IPv6 check box for MGMT under DNS Interfaces.

8. In the General -> Advanced tab, select one of the following from the Send queries from and the Send notify messages and zone transfer requests from drop-down lists:

   - **VIP:** The appliance uses the IP address of the HA port as the source for queries, notifies, and zone transfer requests.
   - **MGMT:** The appliance uses the IP address of the MGMT port as the source for queries, notifies, and zone transfer requests.
   - **LAN2:** The appliance uses the IP address of the LAN2 port as the source for queries, notifies, and zone transfer requests.
   - **Any:** The appliance chooses which port to use as the source for queries, notifies, and zone transfer requests.

   The Send queries from drop-down list also includes loopback IP addresses that you configured. You can select a loopback address as the source for queries.

9. Save the configuration and click Restart if it appears at the top of the screen.

To see that the appliance now also serves DNS on the MGMT port:

1. From the Data Management tab, select the DNS tab -> Members tab -> Grid_member check box.
2. Expand the Toolbar and click View -> View DNS Configuration.
3. Check that the IP address of the MGMT port appears in the address match list in the listen-on substatement.

**About Lights Out Management**

Infoblox LOM (Lights Out Management) is an implementation of the remote management and monitoring of Infoblox appliances that are LOM ready, such as the Trinzic 1410 and 2010 appliances.

The LOM feature is useful when you want to monitor your platforms remotely or consolidate your data centers. When you monitor your systems remotely, you can avoid issues such as overheating of a problematic system by remotely powering down the system. To conserve energy, you can also power up and down any systems based on service requirements.

You can enable LOM for the entire Grid and override the Grid settings for specific members. You can also configure LOM on independent appliances and HA pairs.

**Note:** You can configure LOM only on appliances that support LOM. This port automatically negotiates a speed of 100 Mbps. Devices connected to the LOM port should be configured to auto-negotiate and not have a fixed speed of 1000 Mbps.

LOM is disabled by default. Before you can configure LOM and remotely manage the appliance, ensure that the IPMI (Intelligent Platform Management Interface) port on your appliance is properly connected to the network. Consider the following security measures before you enable the IPMI interface for LOM:

- Use an authentication method other than the RAKP (Remote Authenticated Key-Exchange Protocol) for the IPMI interface. Any implementation that uses the RAKP can become vulnerable.
- Secure the network to which the IPMI interface is connected. Infoblox recommends that you use a separate and secure network for all IPMI traffic.
- Use strong passwords for all IPMI users. At least 10 random characters are recommended. Attacks are only effective against weak
passwords.

- IPMI is disabled by default. DO NOT enable IPMI on the appliances if it is not being used.

By default, IPMI uses UDP port 623. You can then enable LOM and add LOM users through the Infoblox GUI. When you add LOM users, you can assign them specific roles so they can perform only certain functions. When you add a LOM user, you can configure the user to be an "operator" or a "user" depending on the functions you want the user to perform. An operator can access an appliance remotely and perform the following functions:

- Access the serial console
- Reset the appliance
- Power up and down the appliance
- Monitor system status, such as CPU usage and system temperature

A user role can only monitor system status. Users with this role cannot perform any other functions remotely.

After you set up and configure your appliance, perform the following tasks through Grid Manager to enable LOM and set up LOM users:

1. Enable LOM for the Grid or members that support IPMI, as described in 5801008
2. Add LOM users based on your organizational needs, as described in 5801008.
3. Configure the IPMI network interface on the appliance, as described in 58010085801008
4. After you have configured LOM and set up the IPMI interface, install a utility such as IPMItool on your Linux management system. For information about IPMItool, visit the IPMItool web site at http://ipmitool.sourceforge.net. For the most commonly used commands and examples, see 5801008 5801008.

You can also do the following from Grid Manager after you configure LOM:

- Enable and disabled LOM for the Grid or members, as described in 5801008.
- Modify LOM settings, as described in 5801008.
- View LOM users, as described in 5801008.

### Enabling LOM

Before you can add LOM users and manage Infoblox appliances remotely, you must enable LOM. When LOM is configured for the entire Grid, all members inherit the Grid settings. You can also override the Grid settings for specific members. For an HA pair, you can configure LOM on the node that supports IPMI.

To enable and disable LOM:

1. **Grid**: From the Grid tab, select the Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit.
   **Independent appliance**: From the System tab, select the System Manager tab, expand the Toolbar and click System Properties -> Edit.
   **Member**: From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.

   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the LOM tab, complete the following:
   - **Enable Lights Out Management**: LOM is disabled by default. Select this check box to enable LOM. When LOM is enabled or disabled for the Grid, all members inherit the same setting.

3. Save the configuration.

### Adding LOM User Accounts

You can add up to eight LOM user accounts. Admins must use the configured user name and password to remotely log in to the appliance. Note that when you add LOM user accounts at the Grid level, all members inherit them. You can configure user accounts specific to a member by overriding the Grid accounts. When you click Override to modify the inherited Grid accounts, the appliance creates copies of the Grid level user accounts and saves them at the member level. These are new accounts at the member level and do not affect the Grid accounts or any accounts configured on other Grid members. You can also reset member accounts to the Grid accounts by clicking Inherit. When you do that however, all changes you previously made to the member accounts are lost.

To add a LOM user account:

1. **Grid**: From the Grid tab, select the Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit.
   **Independent appliance**: From the System tab, select the System Manager tab, expand the Toolbar and click System Properties -> Edit.
   **Member**: From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.

   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the LOM tab, complete the following:
   - **User Accounts**: Click the Add icon and complete the following:
     - **Name**: Enter the name of the LOM user account.
     - **Password**: Enter the password for the LOM user account. Note that while the maximum length allowed for the password is 20 characters, Infoblox recommends a maximum LOM password length of 16 due to some hardware platform limitations.
     - **Confirm Password**: Enter the password again. Note that while the maximum length allowed for the password is 20 characters, Infoblox recommends a maximum LOM password length of 16 due to some hardware platform limitations.
     - **Role**: From the drop-down list, select the role for the LOM user account. Operator allows users to perform all supported

Copyright ©2019, Infoblox, Inc. All rights reserved.
LOM related functions. **User** allows admins to only monitor system sensors such as temperature and CPU usage.

- **Disable**: Select this to deactivate the user account but keep a user profile.
- **Click Add** to add the new user account.

3. Save the configuration.

### Configuring the IPMI Network Interface

You must configure the IPMI network interface before you can access the appliance remotely. To configure the IPMI network interface:

1. **Independent appliance**: From the **System** tab, select the **System Manager** tab, expand the Toolbar and click **System Properties -> E dit**.
   - **Member**: From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **Grid_member** check box, and then click the **Edit** icon.
2. In the **LOM** tab, complete the following in the **Network Configuration** table:
   - **Address**: Enter the IPMI interface address here.
   - **Subnet Mask**: Enter the subnet mask for the IPMI interface.
   - **Gateway**: Enter the gateway address for the IPMI interface.
3. Save the configuration.

### Modifying LOM Settings

To modify LOM settings:

1. **Grid**: From the **Grid** tab, select the **Grid Manager** tab, expand the Toolbar and click **Grid Properties -> E dit**.
   - **Independent appliance**: From the **System** tab, select the **System Manager** tab, expand the Toolbar and click **System Properties -> E dit**.
   - **Member**: From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **Grid_member** check box, and then click the **Edit** icon.
   - To override an inherited property, click **Override** next to it and complete the appropriate fields.
2. Modify the following:
   - **Enable Lights Out Management**: LOM is disabled by default. Select this check box to enable LOM. When you enable or disable this for the Grid, all members inherit the same setting.
   - **Network Configuration**: Click the fields in the table to modify the IPv4 address, subnet mask, and gateway address for the IPMI interface. For anHA pair, the appliance displays information only for the nodes that support IPMI. Enter the information for the following fields: **Address**, **Subnet Mask**, and **Gateway**. The **Node** and **LAN Address** fields are read-only, and you cannot modify them. The LAN address is the IPMI interface address.
   - **User Accounts**: Click the **Add** icon to add new LOM users. You can also select an existing LOM user and click the **Edit** icon to modify the user settings, as described in **5801008**.
3. Save the configuration.

### Viewing LOM Users

To view information about LOM users:

1. **Grid**: From the **Grid** tab, select the **Grid Manager** tab, expand the Toolbar and click **Grid Properties -> E dit**.
   - **Independent appliance**: From the **System** tab, select the **System Manager** tab, expand the Toolbar and click **System Properties -> E dit**.
   - **Member**: From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **Grid_member** check box, and then click the **Edit** icon.
   - To override an inherited property, click **Override** next to it and complete the appropriate fields.
2. In the **LOM** tab, Grid Manager displays the following information for each LOM user:
   - **Name**: The name of the LOM user.
   - **Role**: The user role to which the LOM user was assigned. This can be **Operator** or **User**.
   - **Disabled**: Indicates whether the LOM user account is disabled or not. When a LOM user account is disabled, the user cannot access the appliance remotely.

### IPMI Commands and Examples

This section describes some of the most commonly used IPMITool commands and examples. For more information about the IPMI commands and usage, visit the IPMITool web site at [http://ipmitool.sourceforge.net](http://ipmitool.sourceforge.net).

To use IPMI commands, complete the following:

1. Ensure that you have properly enabled and configured LOM and the IPMI network interface.
2. Install IPMItool on a Linux management system. For information, visit the IPMITool web site at [http://ipmitool.sourceforge.net](http://ipmitool.sourceforge.net). Access IMPITool and enter an IPMI command to perform a specific task. The appliance displays the corresponding output. Following are some of the most commonly used IPMI commands and their sample outputs. Note that command outputs vary by appliances. The following sample commands were performed on a Trinzic 1410 appliance. All sample commands in this section use the following syntax:

   `ipmitool -H <LOMIPAddress> -U username -P password -L [OPERATOR/USER] -I lanplus <supported commands>`

---

Copyright ©2019, Infoblox, Inc. All rights reserved.
Command to be Used with Caution

**power reset variant**

Caution: Using this command has the same effect as pulling the power cord off the appliance.

Checking Power Status with User Role

Command:

```
ipmitool -H 10.37.2.70 -U user -P infoblox -L USER -I lanplus power status
```

Command output:

Chassis Power is on

Checking Various Sensors [Temperature, Voltage, FANS, Physical Security, Power supply, OEM] with User Role

Command:

```
ipmitool -H 10.37.2.70 -U user -P infoblox -L USER -I lanplus sensor
```

Command output:

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Value</th>
<th>Unit</th>
<th>Status</th>
<th>Lower Limit</th>
<th>Upper Limit</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Temp</td>
<td>23.000</td>
<td>degrees C</td>
<td>ok</td>
<td>-9.000</td>
<td>79.000</td>
<td></td>
</tr>
<tr>
<td>CPU Temp</td>
<td>0x0</td>
<td>discrete</td>
<td>na</td>
<td>na</td>
<td>na</td>
<td></td>
</tr>
<tr>
<td>FAN 1</td>
<td>10390.000</td>
<td>RPM</td>
<td>ok</td>
<td>215.000</td>
<td>29815.000</td>
<td></td>
</tr>
<tr>
<td>FAN 2</td>
<td>na</td>
<td>RPM</td>
<td>na</td>
<td>na</td>
<td>na</td>
<td></td>
</tr>
<tr>
<td>FAN 3</td>
<td>9835.000</td>
<td>RPM</td>
<td>ok</td>
<td>215.000</td>
<td>29815.000</td>
<td></td>
</tr>
<tr>
<td>FAN 4</td>
<td>11870.000</td>
<td>RPM</td>
<td>ok</td>
<td>215.000</td>
<td>29815.000</td>
<td></td>
</tr>
<tr>
<td>FAN 5</td>
<td>10390.000</td>
<td>RPM</td>
<td>ok</td>
<td>215.000</td>
<td>29815.000</td>
<td></td>
</tr>
<tr>
<td>CPU Vcore</td>
<td>0.832</td>
<td>Volts</td>
<td>ok</td>
<td>0.640</td>
<td>1.472</td>
<td></td>
</tr>
<tr>
<td>+3.3VCC</td>
<td>3.264</td>
<td>Volts</td>
<td>ok</td>
<td>2.816</td>
<td>3.712</td>
<td></td>
</tr>
<tr>
<td>+12V</td>
<td>11.978</td>
<td>Volts</td>
<td>ok</td>
<td>10.494</td>
<td>13.303</td>
<td></td>
</tr>
<tr>
<td>CPU DIMM</td>
<td>1.528</td>
<td>Volts</td>
<td>ok</td>
<td>1.152</td>
<td>1.792</td>
<td></td>
</tr>
<tr>
<td>+5V</td>
<td>5.088</td>
<td>Volts</td>
<td>ok</td>
<td>4.096</td>
<td>5.632</td>
<td></td>
</tr>
<tr>
<td>-12V</td>
<td>-12.486</td>
<td>Volts</td>
<td>ok</td>
<td>-13.844</td>
<td>-10.546</td>
<td></td>
</tr>
<tr>
<td>VBAT</td>
<td>3.120</td>
<td>Volts</td>
<td>ok</td>
<td>2.816</td>
<td>3.712</td>
<td></td>
</tr>
<tr>
<td>+3.3VSB</td>
<td>3.264</td>
<td>Volts</td>
<td>ok</td>
<td>2.816</td>
<td>3.712</td>
<td></td>
</tr>
<tr>
<td>AVCC</td>
<td>3.264</td>
<td>Volts</td>
<td>ok</td>
<td>2.816</td>
<td>3.712</td>
<td></td>
</tr>
<tr>
<td>Chassis Intru</td>
<td>0x0</td>
<td>discrete</td>
<td>na</td>
<td>na</td>
<td>na</td>
<td>PS Status : 0x1 discrete : 0x01ff</td>
</tr>
</tbody>
</table>

Printing System Event Log with User Role

Command:

```
ipmitool -H 10.37.2.70 -U user -P infoblox -L USER -I lanplus sel list
```

Command output: The appliance displays all event log entries (if any)

Getting FRU Information with User Role

Command:

```
ipmitool -H 10.37.2.70 -U user -P infoblox -L USER -I lanplus fru
```

Command output:

FRU Device Description : Built-in FRU Device (ID 0) Board Mfg Date : Sun Dec 31 15:00:00 1995
Board Mfg : Supermicro Board Serial : Product Serial :

Powering Off the Appliance with Operator Role

Command:

```
ipmitool -H 10.37.2.70 -U operator -P infoblox -L OPERATOR -I lanplus power off
```

Command output:

Chassis Power Control: Down/Off
Powering On the Appliance with Operator Role

Command:
```
ipmitool -H 10.37.2.70 -U operator -P infoblox -L OPERATOR -I lanplus power on
```
Command output:
```
Chassis Power Control: Up/On
```

Activating the Serial Console Port using Operator role

Command:
```
ipmitool -H 10.37.2.70 -U operator -P infoblox -L OPERATOR -I lanplus sol activate
```
Command output:
```
(64bit) Copyright (c) 1999-2012 Infoblox Inc. All Rights Reserved. type 'help' for more information
Infoblox >
```

Setting Static Routes

When you put the NIOS appliance on a segment of the network where there is a single path to and from it, a single default route is sufficient. For example, in Figure 8.10, the appliance is in the DMZ behind a firewall and connects to the rest of the network through the DMZ interface on the firewall. For example, when hosts send DNS queries from the Internet and the internal network to the appliance and when the appliance replies to those hosts, the firewall takes care of all the routing.

**Note:** This feature is not supported on vNIOS Grid members for Riverbed.

---

**Figure 8.10 Single Default Route**

When the NIOS appliance is on a segment of the network where there are multiple gateways through which traffic to and from the appliance can flow, a single default route is insufficient. For an example, see Figure 8.11.
To resolve the problem illustrated in Figure 8.11, add a second route pointing traffic destined for 10.1.1.0/24 to use the gateway with IP address 1.2.2.2 on firewall 2. This is shown in Figure 8.12.

Figure 8.12 Properly Routed DNS Replies
Whenever you want the NIOS appliance to send traffic through a gateway other than the default gateway, you need to define a separate route. Then, when the appliance performs a route lookup, it chooses the route that most completely matches the destination IP address in the packet header.

When you enable the MGMT port, the gateway you reference in a static route determines which port the NIOS appliance uses when directing traffic to a specified destination.

- If a route definition references a gateway that is in the same subnet as the IP and VIP addresses of the LAN (or LAN1) and HA ports, the NIOS appliance uses the LAN (or LAN1) or HA port when directing traffic to that gateway.
- If a route definition references a gateway that is in the same subnet as the MGMT port, the NIOS appliance uses the MGMT port when directing traffic to that gateway.

*Figure 8.13 Static Routes for the LAN and MGMT Ports*
The need for routes can apply to any type of traffic that originates from the appliance, such as DNS replies, DHCP messages, SNMP traps, ICMP echo replies, Infoblox GUI management, and Grid communications.

To set a static route, do the following:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.
2. In the Network -> Advanced tab of the Grid Member Properties editor, click the Add icon for the IPv4 Static Routes table, and then enter the following:
   - **Network Address**: Type the address and netmask of the remote network to which the NIOS appliance routes traffic.
   - **Gateway Address**: Type the IP address of the gateway on the local subnet through which the NIOS appliance directs traffic to reach the remote network. The gateway address must meet the following requirements:
     - It must belong to a working gateway router or gateway switch.
     - It must be in the same subnet as the NIOS appliance.

   **Note**: Consult your network administrator before specifying the gateway address for a static route on the appliance. Specifying an invalid gateway address can cause problems, such as packets being dropped or sent to an incorrect address.

3. Save the configuration and click Restart if it appears at the top of the screen.

**Defining IPv6 Static Routes**

Principles and applications related to IPv4 static routing in this section apply equally to IPv6. In Figure 8.14, a NIOS appliance supports both IPv4 and IPv6 on its LAN1 port. IPv6 is routed to the internal network while the default IPv4 route remains to the outbound 10.2.2.1 address.

You can use prefix notation to enter an IPv6 network address; the full 128-bit gateway value must be entered. To set an IPv6 static route, do the following:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.
2. In the Network -> Advanced tab of the Grid Member Properties editor, click the Add icon for the IPv6 Static Routes table, and then enter the following:
   - **Network Address**: Type the prefix and prefix length of the remote network to which the NIOS appliance routes traffic. As an example: 2001:DB8::256/64. The double colon is required at the end of the prefix. NIOS performs validity checks on the address.
2. While it is being entered:

- **Gateway Address**: Type the IP address of the gateway on the local subnet through which the NIOS appliance directs traffic to reach the remote network. As an example: 2001:DB8::256:ABCD:EF12:1234:1. The gateway address must meet the following requirements:
  - It must belong to a working gateway router or gateway switch.
  - It must be in the same subnet as one of the interfaces of the NIOS appliance.
  - The gateway address cannot be the same value as that for the VIP.

  **Note**: Consult your network administrator before specifying the gateway address for a static route on the appliance. Specifying an invalid gateway address can cause problems, such as packets being dropped or sent to an incorrect address.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

---

**Figure 8.14 Static Routes for IPv6 Traffic**

---

**Enabling DNS Resolution**

You can specify a network server to perform domain name queries and specify up to two name servers for resolving a DNS name. You can specify the IP address of a preferred name server and that of an alternate name server, plus use a search list for performing partial name resolution.

To enable DNS resolution for a Grid or for an independent appliance or HA pair:

1. **Grid**: From the **Grid** tab, select the **Grid Manager** tab, expand the Toolbar and click **Grid Properties** -> **Edit**.

Member: From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **Grid_member** check box, and then click the Edit icon.

To override an inherited property, click **Override** next to it and complete the appropriate fields.

2. In the **Grid Properties or Member Properties** editor, select the **DNS Resolver** tab, and then enter the following:

- **Enable DNS Resolver**: Select the check box to enable the NIOS appliance to send DNS queries to the preferred or alternate name servers whose IP addresses you specify in the following fields.

Click the Add icon and enter the IP addresses (IPv4 or IPv6) of the servers to which the appliance sends queries. The appliance attempts to resolve the DNS name based on these servers in the order specified.
to send queries to the servers in the order they are listed if it does not receive a response from a listed name server. To move a server up or down on the list, select it and drag it to its new location or click the up and down arrows.

- **Search List**: You can define a group of domain names that the NIOS appliance can add to partial queries that do not specify a domain name. For example, if you define a RADIUS authentication home server as "as1", and you list "corpxyz.com" and "hq.corpxyz.com" in the domain group list, then the NIOS appliance sends a query for "as1.corpxyz.com" and another query for "as1.hq.corpxyz.com" to the preferred or alternate name server. To specify domain names containing IDNs, manually convert it into punycode and specify domain names in punycode.

To add a domain name, click the Add icon and type a domain name in the Search List field. To remove a domain name from the group, select it, and then click **Delete**.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

### Managing Licenses

You must install valid licenses for services and features to function properly in your Infoblox Grid. Licenses are classified by types, as described in **License Types**. You can choose to obtain licenses for the desired features and services and install them as static, dynamic, or Grid-wide licenses, depending on your network and business requirements.

After you install your licenses, you can monitor them through Grid Manager. NIOS displays licenses that are currently active. It also displays the number of licenses that have expired and those that are expiring within the next 30 and 90 days respectively. Click **View Licenses** to view the list of licenses. For information, see **Viewing Member Licenses**.

NIOS licenses are valid for SOT (Son Of Trinzic) 2016 hardware appliances, both physical and virtual. A NIOS license can be permanent or have an expiration date.

#### License Types

Infoblox licenses are divided into the following classes:

- **Static**: Static licenses are member specific. They are installed and tied to the Grid Master or specific Grid members. Static licenses are mapped to the hardware ID for each individual NIOS or vNIOS appliance. For more information about how to obtain and install static licenses, see **Managing Static Licenses**.

- **Dynamic**: These are floating licenses that are dynamically allocated to specific Grid members in the Grid. Dynamic licenses belong to a license pool, which is associated with the entire Grid. When not in use, they can be released back to the pool of licenses for further allocation. In an environment, such as a CMP (Cloud Management Platform), where you need to spin up multiple remote vNIOS appliances at different times based on business requirements, you can consider installing dynamic licenses. For more information about dynamic licenses and how to use them to pre-provision vNIOS appliances, see **Managing Dynamic Licenses** and The table below provide a information about the IB-FLEX platform and various flavor settings.

- **Grid-wide**: Grid-wide licenses are associated with the entire Grid. They are not tied to any particular member. When installed, Grid-wide licenses are replicated to all members in the Grid. Although a Grid-wide license entitles all Grid members to run a particular feature, other conditions and factors determine whether the feature can be enabled on a particular member. For example, a member might not be able to run the Reporting and Analytics feature because it does not have the reporting appliance model. The currently supported Grid-wide licenses are Security Ecosystem, Reporting Subscription, RPZ, Flex Grid Activation and Fire Eye. For more information, see **Managing Grid-wide Licenses**. To configure Grid-wide licenses for RPZ, see **Grid-wide licenses for RPZ**.

In terms of license duration, all static, dynamic, and Grid-wide licenses can have one of the following terms of duration:

- **Perpetual**: Perpetual licenses are permanent licenses that do not have any expiration dates.
- **Non-perpetual**: All non-perpetual licenses have an expiration date, depending on your subscription and the duration of the temporary status.
  - **Subscription** licenses: You must purchase subscription based licenses from Infoblox to use relevant features. After you buy subscription based licenses, you can use those features for a specified period. You can enable one of several sets of subscription through the Grid Manager. These licenses are Grid-wide licenses and are non-perpetual licenses. For more information, see **Subscription Licensing**.
  - **Temporary** licenses: You can enable one of several sets of temporary service licenses through the CLI command set `temp_license`. They provide licensed features and functionality for the interim, while you wait for your permanent licenses to arrive. However, you can subscribe to licenses again after they expire. Note that pool licenses are not supported as temporary licenses.

Before any non-perpetual (subscription or temporary) licenses expire, an expiration warning appears during the GUI login process. The warning reappears during each login until you renew the license. To renew a license, contact your Infoblox representative or Infoblox Technical Support.

**Note**: Grid Manager does not distinguish between subscription and temporary licenses.

### Managing Static Licenses

Static licenses are individual licenses that are tied to specific hardware IDs, and they cannot be transferred among appliances. Static licenses come pre-installed on physical NIOS appliances according to the software packages you order at the time of purchase. You can also obtain static licenses for your vNIOS virtual appliances. Static licenses are specific to a member. For information about how to obtain static licenses, see **Obtaining Static Licenses**. For information about how to add static licenses, see **Adding Permanent or Subscription Licenses**.

Static licenses can be perpetual or non-perpetual. A perpetual license does not have an expiration date. When you install a new static license with
an expiration date beyond the existing license, it replaces the existing license. After you install static licenses on the appliance, you can view their status in Grid Manager, as described in Viewing Licenses.

Obtaining Static Licenses

When you receive a new license key for a static license, it is in CSV (comma separated values) format with the following information: serial number, hardware ID, license type, end date, and license string.

For a static license, you can either upload the license file to the appliance or copy the information and paste it in the text field of the Licenses tab -> Member tab of the Infoblox GUI. You must copy the entire string—serial number, hardware ID, license type, end date, and license string—and save it to the text field. For more information, see Adding Permanent or Subscription Licenses.

To obtain permanent static licenses from Infoblox:

1. After you have set up or pre-provisioned a physical appliance or vNIOS virtual appliance, either log in to the NIOS CLI or open a terminal session for the VM and open the NIOS command line.
2. Run the command `show hwid`. Following is an example:
   ```
   nios-vm-ib-1420-gm > show hwid
   Hardware ID: 564d41e13a1cc55affb9bad4e3b5c48a
   ```
   Copy and paste the Hardware ID value for convenience.
3. You can also run a `show license` command to obtain the same information:
   ```
   nios-vm-ib-1420-gm > show license
   Version : 6.11.0-248090
   Hardware ID : 564d41e13a1cc55affb9bad4e3b5c48a
   ```

   **Note:** Make a note of the hardware IDs that you obtain during this procedure. Each of these unique Hardware ID values can be associated with a Registration Number from your Contract Notification email. If a license key is installed for the current VM, that key value also appears in the output for the show license command.

4. Go to [https://support.infoblox.com/app/licenses](https://support.infoblox.com/app/licenses) (you have to log in with your support account) and click the Licenses menu. On the Licenses page, open Submit a license key registration form.
5. Enter or copy and paste the serial number and hardware ID value for a physical appliance. For a vNIOS appliance, use the hardware ID for both the Serial Number and Hardware ID fields—they are synonymous.
6. Under the Service and Maintenance categories, select the check boxes for all options for which you have purchased service licenses and/or maintenance licenses.
7. Enter any Comments if needed.
8. Click Submit to submit the request for your license keys.

Repeat this procedure for all NIOS and vNIOS appliances in your contract.

Infoblox Technical Support normally processes license key requests on the same day they are received; however, allow 24-48 hours for processing. When you receive the license keys, install the licenses as described in Adding Permanent or Subscription Licenses.

**Note:** Each VM Registration Number should have a Hardware ID associated with it. As you install and spin up each virtual machine, establish written records for each Hardware ID with the VM Registration Numbers in a one-to-one ratio. These value pairs are necessary should you need to contact Infoblox Technical Support.

Obtaining License Keys for Existing Appliances

If you are unsure of the license entitlements for one or more of your NOIS and vNIOS appliances, or want to obtain a new listing of your license keys for any reason, do the following:

1. Go to [https://support.infoblox.com/app/licenses](https://support.infoblox.com/app/licenses) (you have to log in with your support account) and click the Licenses menu. On the Licenses page, open Download License Key(s) for one appliance.
   This feature recognizes that any vNIOS appliance is likely to have multiple feature licenses, all of which are tied to a specific Hardware ID.
2. Enter the Hardware ID number in the Enter one number: field. Following is an example:
3. Select how your license key will be provided:

- Display to Screen
- Send File
- .CSV

The Display to Screen and Send File options allow for direct copying and pasting. Using a .CSV file enables you to use the convenient Upload License File feature for your appliance in NIOS. For more information, see Adding Permanent or Subscription Licenses.

4. After making your selection, click Generate Keys at the bottom of the panel. Following is an example:

**Licenses**

| Serial number or hardware ID: 564d41e13a1cd55defb7bad6413b548a |
|-------------------------|---------------------------|--------------------------|-----------------|------------------|
| **Serial Number**       | **Hardware ID**           | **Entitlement**          | **Expiration**  | **Key**          |
| VM-SHAMMERMAN-01        | 564d41e13a1cd55defb7bad6413b548a | DHCP                    | 2017-04-20      | 00:00:00        |
| VM-SHAMMERMAN-01        | 564d41e13a1cd55defb7bad6413b548a | DNS                     | 2017-04-20      | 00:00:00        |
| VM-SHAMMERMAN-01        | 564d41e13a1cd55defb7bad6413b548a | Grid                    | 2017-04-20      | 00:00:00        |
| VM-SHAMMERMAN-01        | 564d41e13a1cd55defb7bad6413b548a | nHOE (model: FB-1840)   | 2017-04-20      | 00:00:00        |
| VM-SHAMMERMAN-01        | 564d41e13a1cd55defb7bad6413b548a | NOS Maintenance         | 2017-04-20      | 00:00:00        |

5. After you receive your key values, you can save them for your records. To install a specific license or licenses, see Adding Permanent or Subscription Licenses.

**Downloading License Keys for Multiple Appliances**

The Infoblox Technical Support site provides a method for downloading the license keys for multiple VM instances, based on the purchased feature licenses for your products.

1. Obtain the Hardware ID values. Do this in the order shown from top to bottom of your Contract Notification email. As an alternative, you may use the VM Registration Numbers in your Contract Notification email, also separated by commas.
2. Go to https://support.infoblox.com/app/licenses (you have to log in with your support account) and click the Licenses menu. On the Licenses page, open Download License Key(s) for multiple appliances.
3. Enter (or copy and paste) each of the Hardware ID values or VM Registration Numbers into the entry field, each in its own row, with a comma at the end of the value. Do not press Return between each value. An example, using VM Registration Numbers:
4. Click **Generate Keys** at the bottom of the panel (you may need to scroll down to see it).
   The list of keys may be quite substantial. The list shows the license entitlements and registration keys for all vNIOS VMs that are purchased and listed with Infoblox Technical Support.

5. After you receive your key values, you can save them for your records. To install a specific license or licenses, see **Adding Permanent or Subscription Licenses**.

**Managing Dynamic Licenses**

Dynamic licenses are multiple licenses you obtain for NIOS appliances, both physical and virtual. You can install dynamic licenses in advance for different services and features and deploy them on-demand based on your business needs. The appliance stores these licenses in their respective license pools and allocate them when you deploy vNIOS virtual appliances. When you remove a vNIOS appliance from your Grid, the applicable licenses are automatically released back to the license pool. The appliance adjusts the total number of licenses accordingly. You can use dynamic licenses to automatically pre-provision and deploy vNIOS appliances. For more information about this feature, see **About Elastic Scaling**.

For a dynamic license, you can either upload the license file to the appliance or copy the information and paste it in the text field of the **Licenses** tab of the Infoblox GUI. You must copy the entire string and save it to the text field. When you restore or perform a factory reset operation, you will lose the existing dynamic licenses.

License pools for a particular license type are an aggregate of the subpools that contains the respective license type. Subpools are either perpetual or non-perpetual with different expiration dates. NIOS displays non-perpetual and perpetual subpools with different expiration dates within the same pool.

Dynamic licenses can be allocated from a pool based on the aggregate install count. You can allocate licenses from a pool as long as the allocated count of perpetual and non-perpetual licenses does not exceed the count of perpetual and active non-perpetual licenses that are installed.

**Note:** You must install both the **Enterprise** (formerly Grid) and vNIOS licenses on a vNIOS appliance for it to join the Grid. You can add other licenses such as DNS, DHCP, or Cloud Platform depending on how you deploy your vNIOS virtual appliances.

**Obtaining Dynamic Licenses**

When you purchase licenses for specific features and services, you may deploy the licenses as dynamic licenses. License information is stored in a license file with the following information for each license: LSN-P (License Serial Number - Proxy), LK-P (License Key Proxy), LSN (License Serial Number) and LK (License Key). License keys are generated based on the LPC_UID (License Pool Container Unique ID) of the Grid Master. You must first obtain the LPC_UID of the Grid, also called the Grid license UID from the Grid Master and then contact Infoblox Technical Support to obtain dynamic licenses.

Infoblox stores information related to dynamic licenses in a license file. When you install dynamic licenses, you must upload the entire license file to the Grid Master, as described in **Adding Permanent or Subscription Licenses**.

To obtain dynamic licenses:

1. Log in to Grid Manager and obtain the LPC_UID from the Grid Master, as follows:
   a. From the **Grid** tab, select the **Licenses** tab -> **Pool** tab, and then click **Export All Licenses** from the Toolbar.
   b. Save the CSV file.
   c. Open the CSV file. The LPC_UID is displayed in the **SIGNATURE** row. Copy this ID. You will need this ID when contacting Infoblox Technical Support.

   **Note:** You can also use the show license_pool_container CLI command to display the LPC_UID.

2. Contact Infoblox Technical Support or your Infoblox representative to obtain the dynamic licenses.
Manually Allocating Dynamic Licenses

To allocate a particular feature license to a NIOS member:

1. From the Grid tab, select the Licenses tab -> Pool tab.
2. Select the feature license and click the Action icon (shown as a gear in each row for the table) next to the license, and then select Allocate from the list.
3. In the Allocate Pool Licenses dialog, click Select Member Node.
4. From the Member Selector, click the FQDN of the NIOS member on which you want to install the feature license. The appliance displays the member in the To this member: field.
5. Click Allocate to install this license on the selected member or click Cancel to cancel this action.

NIOS allocates the license and adjusts the numbers in the Assigned and Available fields in the Pool tab.

Manually Deallocating Dynamic Licenses

To deallocate a particular feature license from a NIOS member:

1. From the Grid tab, select the Licenses tab -> Member tab.
2. Select the license and click the Action icon (shown as a gear in each row for the table) next to the license, and then select Deallocate from the list.
3. In the Deallocate Pool Licenses dialog, select the license(s) you want to deallocate from the Pool Licenses table.
4. Click Deallocate to remove the license(s) from the member(s) or click Cancel to cancel this action.

NIOS deallocates the license from the respective members and adjusts the numbers in the Assigned and Available fields in the Pool tab.

Manually Revoking Dynamic Licenses

To remove a particular feature license from the pool:

1. From the Grid tab, select the Licenses tab -> Pool tab.
2. Select the feature license and click the Action icon (shown as a gear in each row for the table) next to the license, and then select Revoke from the list.
3. In the Remove Licenses dialog, click the Number field and enter the number of licenses you want to remove for the selected license type.
4. Click Remove Licenses to remove the license(s) or click Cancel to cancel this action.

NIOS removes the license(s) and adjusts the numbers in the Assigned and Available fields in the Pool tab.

Managing Grid-wide Licenses

NIOS supports Grid-wide licenses that are valid across the entire Grid. You can obtain Grid-wide licenses for the following features: Security Eco system, Reporting Subscription, RPZ, Flex Grid Activation and FireEye. Although a Grid-wide license entitles all Grid members to run a particular feature, other conditions and factors determine whether the feature can be enabled on a particular member. For example, a member might not be able to run the Reporting and Analytics feature because it does not have the reporting appliance model. For more information about obtaining Grid-wide licenses, see Obtaining Grid-wide Licenses.

For a Grid-wide license, you can either upload the license file to the appliance or copy the information and paste it in the text field of the Licenses tab -> Grid Wide tab of Grid Manager. You must copy the entire string (license type, expiry date, and license string) and save it to the text field.

The Flex Grid Activation license is bundled with the following licenses: Grid (enterprise), Unbound, DCA, DNS, the DTC, Software Threat Protection, Threat Protection Update, DNSFW, NXDOMAIN Redirect, FireEye, Threat Analytics and Security Ecosystem. For more information about Flex Grid Activation license, see About the Flex Grid Activation License.

Note the following about Grid-wide licenses:

- When you restore or perform a factory reset operation, you will lose the existing Grid-wide licenses.
- NIOS restores any Grid-wide licenses that are present in a restored database.
- When you restore a database from another Grid, NIOS replaces the UID of the Grid and the Grid-wide licenses from the other Grid.
- Static and Grid-wide licenses of the same type can co-exist in the same Grid.
- If a member is pre-provisioned for a specific feature, it is allowed to join the Grid that has the Grid-wide license for that feature even if the member does not have a license for that feature.

About the Flex Grid Activation License

Infoblox introduces a permanent license called Flex Grid Activation that you can implement as a NIOS Grid-wide license to enable the following
features at the same time: Grid (enterprise), Unbound, DCA, DNS, the DTC, Software ADP, Threat Protection Update, DNSFW, NXDOMAIN Redirect, FireEye, Threat Analytics and Security Ecosystem. This license is valid for IB-FLEX members only. For more information, see About IB-FLEX. After you install the Flex Grid Activation license, you can view it in the Grid tab -> Licenses tab -> Grid Wide tab of Grid Manager. For more information, see Managing Grid-wide Licenses.

You can install the Flex Grid Activation license on a Grid Master even if IB-FLEX is not a part of the Grid, but this license is effective only for an IB-Flex member. The Infoblox License Portal allows you to acquire any number of Flex Grid Activation license keys for each individual Grid. To install a temporary license, use the set temp_license CLI command. For more information about this command, refer to the Infoblox CLI Guide.

Obtaining Grid-wide Licenses

When you purchase licenses for specific features and services, the licenses may be Grid-wide licenses. License information is stored in a license file with the following information for each license: LSN-P (License Serial Number - Proxy), LK-P (License Key Proxy), LSN (License Serial Number) and LK (License Key).

License keys are generated based on the license UID of the Grid Master. You must first obtain the UID of the Grid and then contact Infoblox Technical Support to obtain the Grid-wide licenses.

**Note:** Ensure that you obtain the license UID of the Grid Master. If you use the license UID of a Grid member or an appliance that has not yet joined the Grid, you might not be able to properly install the Grid-wide license.

The license file (CSV) format for Grid-wide licenses are as follows:

```
GRID_WIDE,license_uid,license_type,[expiry_date],license_string
```

Infoblox stores information related to Grid-wide licenses in a license file. When you install Grid-wide licenses, you must upload the entire license file to the Grid Master, as described in Adding Permanent or Subscription Licenses.

To obtain Grid-wide licenses:

1. Log in to Grid Manager and obtain the license UID from the Grid Master, as follows:
   a. From the Grid tab, select the Licenses tab -> Grid Wide tab, and then click Export All Licenses from the Toolbar.
   b. Save the CSV file.
   c. Open the CSV file. The UID is displayed in the SIGNATURE row. Copy this ID. You will need this ID when contacting Infoblox Technical Support.

   **Note:** To obtain the UID of the Grid, you can use the show license_uid CLI command on the Grid Master. For more information, refer to the Infoblox CLI Guide.

2. Contact Infoblox Technical Support or your Infoblox representatives to obtain the Grid-wide licenses.

Adding Permanent or Subscription Licenses

To add permanent or subscription licenses:

1. From the Grid tab, select the Licenses tab -> Member tab or Pool tab or Grid Wide tab and click the Add icon.
2. Do one of the following:
   a. **Upload License File:** You must use this method to upload dynamic licenses and Grid-wide licenses. Click Select File and navigate to the license file.
   b. **Paste License(s):** Paste the license key in this text field. You must paste the entire string in CSV format: serial number, hardware ID, license type, end date, and license string. If you are pasting multiple licenses, start each string on a new line.
3. Click Save License(s).
   The appliance validates the license and adds it to the table. Close the browser window and log in to the Infoblox GUI. If you are activating licenses for an HA pair, you must follow this procedure for both nodes.

**Note:** To transfer licenses between vNIOS on VMware appliances, refer to the Infoblox Installation Guide for vNIOS Software on VMware.

Adding Temporary Licenses

You can use the CLI command set temp_license to generate and install temporary licenses. This can provide licensed features and functionality for the interim, while you wait for your permanent license to arrive.

To generate a temporary license:

1. Log in to the NIOS appliance through a remote console window. For more information on how to open a remote console window, refer to the Infoblox CLI Guide.
2. At the Infoblox command prompt, enter **set temp_license**. The appliance lists the available licenses, and you select those you need.
3. Enter the number of the licenses you want to install.
4. Confirm the selection when prompted, and the following message appears:
   - Temporary license is installed.
### Viewing Licenses

If the appliance is part of a Grid, you must log in to the Grid Master to view license information from Grid Manager. If the appliance is an independent appliance, log in to System Manager on the appliance. If you have transferred licenses from one vNIOS appliance to another, you can view information about the new and replaced licenses.

Grid Manager displays licenses in the **Grid** tab -> **Licenses** tab. You can view license information for all static and dynamic licenses, including temporary licenses, in the **Member** tab, and a summary of dynamic licenses in the **Pool** tab. For more information, see [Viewing Member Licenses](#).

### Viewing Member Licenses

To view information about active licenses, including static and dynamic licenses that are currently assigned or allocated to NIOS and vNIOS appliances:

1. Log in to Grid Manager on the Grid Master or System Manager on an independent appliance.
2. Select the **Grid** or **System** tab -> **Licenses** tab -> **Member** tab. The appliance displays the following information:

   - **Type of License**: The license category. This can be **Static**, **Dynamic**, **Grid Wide**, or **Paid NIOS**. Static licenses are individual licenses you obtain and are currently assigned to specific appliances. These licenses are tied to specific hardware IDs and you cannot deallocate them. Dynamic licenses are pooled licenses that support the Elastic Scaling feature, which enables central tracking, granting, and management of NIOS feature licenses for vNIOS entities in the Grid. You can manually allocate and deallocate dynamic licenses. For information about Elastic Scaling, see [The table below provides information about the IB-FLEX platform and various flavor settings](#). When installed, Grid-wide licenses are replicated to all members in the Grid. The currently supported Grid-wide licenses are [Security Ecosystem, Reporting Subscription, RPZ, Flex Grid Activation and FireEye](#).

   - **Paid NIOS represents the pay-as-you-go licensing model for vNIOS virtual appliances. In the AWS Marketplace, when you use the Paid NIOS model to launch the vNIOS for AWS virtual appliance, the virtual appliance comes pre-installed with the following permanent licenses: vNIOS, Grid, DNS, and CNA](#). As long as the virtual appliance is up and running, you can use the NIOS features that these licenses provide. You cannot add, delete, import, or export Paid NIOS licenses. For information about the Paid NIOS in AWS Marketplace, refer to the [Installation Guide for vNIOS for AWS](#).

   - **Feature**: Indicates the features for which the license was installed. For example, if the license was installed for DNS service, this shows DNS.

   - **Name**: The FQDN of the appliance.

   - **HA**: Indicates whether the appliance is an HA pair.

   - **IPv4 Address**: The IPv4 address of the appliance, if applicable.

   - **IPv6 Address**: The IPv6 address of the appliance, if applicable.

   - **Hardware ID**: The unique hardware ID of the appliance. The ID is highlighted in red if the license on the appliance was removed.

   - **Serial Number**: The serial number of the appliance.

   - **Type Context**: Depending on the license type, this field displays the attribute (such as **Model** that the license controls. This field is blank if the license does not control any attribute type. This field can display one of the following:

     - **Leases**: Indicates that this DHCP license supports a specific number of DHCP leases. The number of leases supported is displayed in the **Type Details** field.

     - **Model**: Indicates that this vNIOS license supports a specific vNIOS virtual appliance model. The model supported is displayed in the **Type Details** field.

     - **Tier**: Indicates various levels of performance limits on the DNS cache acceleration license of the Infoblox-4030 appliance. This is only applicable to the Infoblox-4030 appliance.

   - **Type Details**: Information about the attribute type that the license monitors. This field can display the following information for each attribute:

     - **Leases**: The number of DHCP leases that the DHCP license supports.

     - **Model**: The model of the NIOS virtual appliance license, such as IB-V1410 or IB-V2215.

     - **Tier**: The performance limit value of an Infoblox-4030 appliance with DNS Cache Acceleration, such as Tier-1 for full capacity (up to 1M qps), Tier-2 for high (up to 600K qps), Tier-3 for base (up to 300K qps) performance limits, and Tier-4 (up to 150K qps). This is only applicable to the Infoblox-4030 appliance.

   - **Expiration**: The expiration date of the license.

   - **Replaced Hardware ID**: The hardware ID of the appliance whose license was removed.

### Viewing Dynamic Licenses

You can install dynamic licenses on the Grid Master for future vNIOS appliance deployments. When you install dynamic licenses, the Grid Master store them in a license pool. You can view these licenses and evaluate license usage for vNIOS virtual appliances.

For a particular feature, such as DNS or DHCP, Grid Manager displays dynamic licenses in sub pools so you can view the number of permanent licenses, the number of licenses that are expiring on a particular date, and those that are expired. NIOS highlights the licenses that are going to expire soon using a yellow background. Licenses that are approaching expiry are highlighted with a pink background.

**Note**: The overall license status for a particular feature reflects the most critical status among all licenses in the pool. For example, if there are expired licenses in the pool, the overall status for this license type appears as expired.

To view dynamic licenses in the pool and their usage information:
1. Log in to Grid Manager on the Grid Master.
2. Select the Grid tab -> Licenses tab -> Pool tab. The appliance displays the following information:
   - **Feature**: The feature for which you have obtained the license.
   - **Installed**: The number of licenses that have been installed for the specified feature.
   - **Assigned**: The number of licenses currently allocated to vNIOS virtual appliances.
   - **Available**: The number of licenses that are currently available for the specified feature.
   - **License Model**: For vNIOS license only. Indicates the model type of the vNIOS virtual appliance. Note that the vNIOS license you install on the vNIOS appliance must match the appliance model. You can use vNIOS license that has a higher capacity on a vNIOS appliance that has a smaller capacity, but not vice versa. For example, you can install a CP-V1400 license on a CP-V800 or CP-V1400 appliance, but not on a CP-V2200.
   - **Limit Context**: Depending on the license type, this field displays the attribute (such as **Model**) that the license controls. This field is blank if the license does not control any attribute type. This field can display one of the following:
     - **Leases**: Indicates that this DHCP license supports a specific number of DHCP leases. The number of leases supported is displayed in the **Type Details** field.
     - **Model**: Indicates that this vNIOS license supports a specific vNIOS virtual appliance model. The model supported is displayed in the **Type Details** field.
     - **Tier**: Indicates various levels of performance limits on the DNS cache acceleration license of the Infoblox-4030 appliance. This is only applicable to the Infoblox-4030 appliance.
   - **Limit Value**: Information about the attribute type that the license monitors. This field can display the following information for each attribute:
     - **Leases**: The number of DHCP leases that the DHCP license supports.
     - **Model**: The model of the vNIOS virtual appliance, such as IB-V410 or IB-V2215.
     - **Tier**: The performance limit value of an Infoblox-4030 appliance with DNS Cache Acceleration, such as Tier-1 for full capacity (up to 1M qps), Tier-2 for high (up to 600K qps), and Tier-3 for base (up to 300K qps) performance limits. This is only applicable to the Infoblox-4030 appliance.
   - **Expiration**: The expiration date and time of the license. It displays **Permanent** for permanent licenses and **Expired** for licenses that expired.

3. Click the arrow mark next to the check box of a specific feature to view the list of licenses and their respective expiration dates.

**Viewing Grid-wide Licenses**

Grid Manager displays the licenses that are configured for the respective Grid. To view Grid-wide licenses:

1. Log in to Grid Manager on the Grid Master.
2. Select the Grid tab -> Licenses tab -> Grid Wide tab. The appliance displays the following information:
   - **Feature**: The feature for which you have obtained the license.
   - **Limit Context**: Depending on the license type, this field displays the attribute (such as **Model**) that the license controls. This field is blank if the license does not control any attribute type. This field can display one of the following:
     - **Leases**: Indicates that this DHCP license supports a specific number of DHCP leases. The number of leases supported is displayed in the **Type Details** field.
     - **Model**: Indicates that this vNIOS license supports a specific vNIOS virtual appliance model. The model supported is displayed in the **Type Details** field.
     - **Tier**: Indicates various levels of performance limits on the DNS cache acceleration license of the Infoblox-4030 appliance. This is only applicable to the Infoblox-4030 appliance.
   - **Limit Value**: Information about the attribute type that the license monitors. This field can display the following information for each attribute:
     - **Leases**: The number of DHCP leases that the DHCP license supports.
     - **Model**: The model of the vNIOS virtual appliance, such as IB-V410 or IB-V2215.
     - **Tier**: The performance limit value of an Infoblox-4030 appliance with DNS Cache Acceleration, such as Tier-1 for full capacity (up to 1M qps), Tier-2 for high (up to 600K qps), and Tier-3 for base (up to 300K qps) performance limits. This is only applicable to the Infoblox-4030 appliance.
   - **Expiration**: The expiration date and time of the license. It displays **Permanent** for permanent licenses.

You can do the following:
- Delete a Grid-wide license. For information, see **Removing Licenses**.
- Click the Export icon to export the list of licenses to a .csv file.
- Click the Print icon to print the list of licenses.

To search for specific licenses in the Member, Pool and Grid Wide tabs, you can use filters and the Go to function (the Go to function is not supported in the Pool tab) to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches. You can also create a quick filter to save frequently used filter criteria. For information, see **Using Quick Filters**.

**Backing Up Licenses**

You can back up all the static licenses, dynamic licenses in the license pool container and Grid-wide licenses, in case you need to re-install them at a later time. Infoblox recommends backing up the licenses before removing any of them.

Copyright ©2019, Infoblox, Inc. All right reserved.
Note: Dynamic licenses are not exported to this file. Dynamic licenses are automatically released and returned to the license pool on the Grid Master when a member leaves the Grid. Unallocated dynamic Licenses are available for allocations.

When you back up the licenses, Grid Manager creates a CSV file that lists the following information for each license: serial number, hardware ID, license type, end date, license string.

To back up licenses:
1. From the Grid tab, select the Licenses tab.
2. Click Export All Licenses from the toolbar. Grid Manager generates a CSV file that contains all the licenses. Depending on the browser you use, you can then open the file or save it to a specified location.

Removing Licenses

You can remove licenses and reset a NIOS appliance to its factory default settings. For example, if you have a NIOS appliance running the DNSone package with the Grid upgrade, but you want to use it as an independent appliance, you can remove the Grid license. Infoblox recommends that you back up licenses before removing them, in case you decide to re-install them at a future time.

When you remove a Grid-wide license, the licensed feature is deactivated on all the members that is affected by the license. On the other hand, when you remove a member from the Grid, the member no longer has the ability to run the feature associated with the Grid-wide license now that it is not part of the Grid.

Note: Exercise caution when removing licenses; you may render an appliance unusable by removing the wrong license. Other feature sets may be affected once you remove a license; for example, removing licensing for DNS and DHCP services will also disable task packs in the NIOS Daemonintestinal boards -> Tasks page.

To remove an active license:
1. From the Grid tab, select the Licenses tab -> Member tab or Grid Wide tab.
2. Select the license and click the Delete icon.
3. Check the license that you are about to remove. Note that removing the wrong license can render an appliance unusable.
4. Close the browser window and log in to the Infoblox GUI.

About IB-FLEX

IB-FLEX is a virtual platform that is scalable based on the resource that you allocate to the virtual machine. NIOS automatically detects the capacity of the virtual machine and scales it to the appropriate platform after you provision the IB-FLEX member.

You must first install the Grid license on a non IB-FLEX appliance that is designated as the Grid Master to allow members to join the Grid, even if you have already installed an Flex Grid Activation license. This license does not affect a non IB-FLEX Grid Master.

An IB-FLEX appliance designated as a member does not require any license, either Grid or vNIOS, while joining the Grid. When you register an IB-FLEX member, the appliance checks for the Grid (enterprise) license and changes it to a non IB-FLEX member. For an IB-FLEX appliance, it checks for an Flex Grid Activation Grid-wide license before node registration.

IB-FLEX members can join the Grid through the MGMT interface when Software ADP is enabled. You can configure an IB-FLEX appliance to function as a Grid Master or a member. To enable reporting for a Grid member that is running Software ADP, you must configure the MGMT interface.

A non IB-FLEX appliance designated as a member requires either a Grid and/or vNIOS/NIOS licenses installed to join the Grid. Similarly, for a reporting appliance to join the Grid, you must install a Grid and/or vNIOS/NIOS licenses. You cannot assign pool licenses to an IB-FLEX appliance. IB-FLEX supports HA for appliances that are running Software ADP.

Infoblox supports elastic scaling on IB-FLEX members that use the Flex Grid Activation Grid-wide license. It also supports pre-provisioning for Software ADP on the supported platforms. You must add the new IB-FLEX model to the list of supported pre-provisioning hardware types, so that you can select it during the member pre-provisioning. To pre-provision a non IB-FLEX Grid member, you must have valid pool licenses and pre-provisioned those members in the Grid.

**IMPORTANT:** To set up a supported virtual appliance as an IB-FLEX, you must first define the hardware type of the virtual appliance as IB-FLEX before you configure it. Depending on the platform or environment in which you are installing IB-FLEX, you can define the hardware_type parameter to IB-FLEX during the cloud-init process, or you can manually set the hardware type using the set hardware-type CLI command. For more information, see set hardware-type.

Limitations of IB-FLEX

- It is not compatible with the traditional node-based licensing and it supports capacity based licensing only.
- An IB-FLEX instance will not start if you do not configure the required minimum level of resources.
- The resources assigned to IB-FLEX for cores and memory must be equal to or exceed the minimum designated values for the platform. For more information about IB-FLEX platforms, see About IB-FLEX Instances and Platform Settings.
- IB-FLEX does not support DNS64 on appliances running NIOS version 8.2.0.
Installing IB-FLEX

Depending on your network environment, you can install IB-FLEX just like how you install other Infoblox virtual appliances. Before you deploy an IB-FLEX, ensure that you set the hardware type of the appliance to IB-FLEX. You can do so either through the cloud-init process during deployment or manually through the set hardware-type CLI command.

You can configure an IB-FLEX only on the following Infoblox appliances:

- IB-1405, IB-1415, IB-1425
- IB-2205, IB-2215, IB-2225
- TE-4015

For more information about installing IB-FLEX in the VMware environment, see Deploying vNIOS Appliances on VMware.

For information about installing IB-FLEX in the OpenStack environment, see Deploying vNIOS for KVM in OpenStack Using Elastic Scaling.

About IB-FLEX Instances and Platform Settings

An IB-FLEX instance supports capacity-based licensing only, but it is compatible with NIOS Grid Master that uses node-based licensing. You can upgrade an IB-FLEX instance from a low-end platform to a high-end platform by increasing the resource allocation of the virtual machine. An IB-FLEX instance selects the default internal settings for a respective instance platform based on the resource settings detected during the startup.

An IB-FLEX instance supports VMware ESXi with or without SR-IOV enabled and OpenStack with KVM both with or without SR-IOV. The table below provides information about the IB-FLEX platform resource specification:

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Allowed Range of Values</th>
<th>Recommended Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual NUMA Nodes</td>
<td>1</td>
<td>1</td>
<td>Single virtual CPU socket</td>
</tr>
<tr>
<td>Disk Size</td>
<td>250 GB</td>
<td>250 GB</td>
<td>Fixed size virtual disk</td>
</tr>
</tbody>
</table>

The table below provides information about the IB-FLEX platform and various platform settings:

<table>
<thead>
<tr>
<th>Intended Use</th>
<th>Total CPU</th>
<th>Total Virtual Memory GB (Without Software ADP)</th>
<th>Total Virtual Memory GB (With Software ADP)</th>
<th>Database Object Count</th>
<th>Grid Master Capable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small Authoritative DNS</td>
<td>4</td>
<td>8</td>
<td>10</td>
<td>100,000</td>
<td>No</td>
</tr>
<tr>
<td>Medium Authoritative DNS</td>
<td>8</td>
<td>16</td>
<td>22</td>
<td>600,000</td>
<td>Yes</td>
</tr>
<tr>
<td>Large Authoritative DNS</td>
<td>16</td>
<td>32</td>
<td>40</td>
<td>16,000,000</td>
<td>Yes</td>
</tr>
<tr>
<td>Recursive DNS (without acceleration)</td>
<td>6</td>
<td>14</td>
<td>18</td>
<td>200,000</td>
<td>Yes</td>
</tr>
<tr>
<td>Large Recursive DNS (without acceleration)</td>
<td>14</td>
<td>28</td>
<td>36</td>
<td>5,000,000</td>
<td>Yes</td>
</tr>
<tr>
<td>Small Grid Master</td>
<td>10</td>
<td>18</td>
<td>26</td>
<td>1,000,000</td>
<td>Yes</td>
</tr>
<tr>
<td>Medium Grid Master</td>
<td>12</td>
<td>22</td>
<td>30</td>
<td>2,000,000</td>
<td>Yes</td>
</tr>
<tr>
<td>Large Grid Master</td>
<td>16</td>
<td>32</td>
<td>40</td>
<td>16,000,000</td>
<td>Yes</td>
</tr>
<tr>
<td>Small Recursive DNS (with acceleration)</td>
<td>8</td>
<td>12</td>
<td>NA</td>
<td>100,000</td>
<td>No</td>
</tr>
<tr>
<td>Medium Recursive DNS (with acceleration)</td>
<td>16</td>
<td>20</td>
<td>NA</td>
<td>100,000</td>
<td>No</td>
</tr>
<tr>
<td>Large Recursive DNS (with acceleration)</td>
<td>26</td>
<td>30</td>
<td>NA</td>
<td>100,000</td>
<td>No</td>
</tr>
</tbody>
</table>

Note the following about IB-FLEX:

- You cannot mark an IB-FLEX appliance as a Grid Master or Grid Master Candidate with resources that are intended for small authoritative DNS, small recursive DNS (with acceleration), medium recursive DNS (with acceleration), and large recursive DNS (with acceleration). For more information, see Table 8.8.
- Infoblox recommends that you increase the memory to the following for IB-FLEX members to use certain features:
  - 16 GB, instead of the standard 14 GB, to use DNS analytics.
  - 20 GB, instead of the standard 18 GB, to use Threat analytics when RPZ is assigned to the IB-FLEX member.
**Configuring DNS Cache Acceleration on IB-FLEX**

When you enable the virtual DNS cache acceleration feature on the IB-FLEX, the appliance acts as a high-speed DNS caching-only name server. This feature provides DNS cache acceleration support for recursive UDP DNS queries on the IB-FLEX. The DNS cache acceleration feature is bundled with the **Flex Grid Activation** license. When you install this license, you are entitled to use the DNS cache acceleration feature on IB-FLEX.

IB-FLEX supports RPZ, but the response for RPZ queries are not cached by the DNS cache accelerator. Instead, these queries are bypassed to the host and you can configure cache expiry period for RPZ queries. Note that the maximum cache lifetime for DNS cache acceleration on IB-FLEX is set to 300 seconds when you configure RPZ zones for a member.

You can also use Elastic Scaling to pre-provision DNS cache acceleration on IB-FLEX. IB-FLEX supports Intel x86_64 systems with IOMMU, Hugepages processors, virtio-net, and Intel 82599 10 G NIC and SRIOV with Intel 82599 ethernet controllers for DNS cache acceleration.

You can configure DNS cache acceleration on IB-FLEX using the Grid Manager or API. To view accelerated cache details, you can either log in to Grid Manager, or use CLI commands, or Infoblox API. Infoblox supports Auto Scaling that contains OpenStack packages to automatically scale the required number of resources based on your application. For more information, refer to [Auto Scaling for Virtual DNS Cache Acceleration](#).

**Note:** Certain features such as DNS64, Sort list, and NIC bonding that are supported on the IB-4030 platform are not supported on IB-FLEX. These features do not work if you replace IB-4030 appliances with IB-FLEX appliances.

Associated characteristics of the IB-FLEX appliance include the following:

- Cache delete through the Grid Manager, CLI or Infoblox API. For more information about cache delete, see [Clearing DNS Cache](#).
- ACL for IPv4 and IPv6.
- Sending SNMP traps for DNS cache acceleration service on IB-FLEX.
- SNMP queries for IB-FLEX.
- Fixed RRSET order for accelerated responses, for A and AAAA record types, for IPv4 and IPv6.
- Both non-accelerated recursive and authoritative DNS with Software ADP.

The table below lists the features that are either supported or not supported on the Software DNS cache acceleration platforms:

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported / Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tiered licensing</td>
<td>Licensing is based on the Flex Grid Activation license on the Grid. Note that the queries per second are limited by the number of CPUs for IB-FLEX.</td>
</tr>
<tr>
<td>RPZ</td>
<td>Yes, the maximum cache lifetime for DNS cache acceleration is set to 300 seconds if RPZ zones are configured for the member.</td>
</tr>
<tr>
<td>Caching (A, AAAA, MX, CNAME, PTR)</td>
<td>Yes</td>
</tr>
<tr>
<td>Do not cache: EDNS, TCP, Any, TSIG</td>
<td>Yes</td>
</tr>
<tr>
<td>Caching over additional interfaces (v4, v6)</td>
<td>Yes</td>
</tr>
<tr>
<td>Dump Acceleration Cache (CLI, GUI, PAPI)</td>
<td>Yes</td>
</tr>
<tr>
<td>Clear Acceleration Cache (CLI, GUI, PAPI)</td>
<td>Yes</td>
</tr>
<tr>
<td>Cache pre-fetch and cache refresh</td>
<td>Yes</td>
</tr>
<tr>
<td>ACLs (Allow-queries/Responses, Match-Clients/Destination, Blackhole)</td>
<td>Yes</td>
</tr>
<tr>
<td>AAAA Filtering (Bypassed but support configuring)</td>
<td>Yes</td>
</tr>
<tr>
<td>Fixed RRSET ordering</td>
<td>Yes</td>
</tr>
<tr>
<td>DNS64</td>
<td>No</td>
</tr>
<tr>
<td>DNS monitoring feature (netmon)</td>
<td>Yes, but unlike IB-4030 this feature captures DNS cached queries on the virtual DNS cache acceleration platform.</td>
</tr>
<tr>
<td>DNS Query logging (BIND only)</td>
<td>Yes</td>
</tr>
<tr>
<td>DNS Views</td>
<td>Yes, supports up to six DNS views.</td>
</tr>
<tr>
<td>Forward/Stub zones</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>Support</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Unbound as DNS resolver</td>
<td>Yes, unbound is supported through the Flex Grid Activation license.</td>
</tr>
<tr>
<td>DNS cache acceleration related restrictions for configuration.</td>
<td>Yes, for NIOS version 8.2.0 restrictions are enforced based on whether the DNS cache acceleration feature is enabled or disabled.</td>
</tr>
<tr>
<td>Reporting</td>
<td>Yes, please see Reports for IB-FLEX.</td>
</tr>
<tr>
<td>VLAN</td>
<td>No, Infoblox does not support VLAN for virtual appliances.</td>
</tr>
<tr>
<td>DSCP</td>
<td>No, Infoblox does not support DSCP for virtual appliances.</td>
</tr>
<tr>
<td>Sort list</td>
<td>No</td>
</tr>
<tr>
<td>Anycast (OSPF and BGP)</td>
<td>Yes</td>
</tr>
<tr>
<td>BFD (Bidirectional Forwarding Detection)</td>
<td>Yes</td>
</tr>
<tr>
<td>HA Support</td>
<td>Valid only for non-SRIOV.</td>
</tr>
<tr>
<td>NIC Bonding</td>
<td>No</td>
</tr>
<tr>
<td>Multiple-Interfaces on same subnet</td>
<td>No</td>
</tr>
<tr>
<td>IP Rate-limit and Response logging</td>
<td>No</td>
</tr>
<tr>
<td>EDNS Client Subnet support</td>
<td>No</td>
</tr>
<tr>
<td>NXDOMAIN redirection</td>
<td>Yes</td>
</tr>
<tr>
<td>DNSSEC (Bypassed but support configuring)</td>
<td>Yes</td>
</tr>
<tr>
<td>Debug enhancements</td>
<td>Yes</td>
</tr>
<tr>
<td>SNMP Support for DCA service related traps</td>
<td>Yes</td>
</tr>
<tr>
<td>SNMP stats support for DNS QPS and CHR</td>
<td>Yes</td>
</tr>
<tr>
<td>NX Mitigation</td>
<td>No</td>
</tr>
<tr>
<td>NetFilter (Tracking tables)</td>
<td>No</td>
</tr>
<tr>
<td>Traffic-capture (All modes)</td>
<td>Yes, partial support. Note that tcpdump captures both queries and responses.</td>
</tr>
<tr>
<td>No flush-mode support for DNS cache acceleration cache</td>
<td>Yes</td>
</tr>
<tr>
<td>Per-interface UDP DNS cache acceleration response counters</td>
<td>Yes</td>
</tr>
<tr>
<td>CLI commands</td>
<td>You can use the commands set dns-accel and show dns-accel to view and set DNS cache acceleration information. For more information, refer to the Infoblox CLI Guide.</td>
</tr>
<tr>
<td>DNS Query rewrite (Bypassed but supports configuring)</td>
<td>No</td>
</tr>
<tr>
<td>Threat Protection</td>
<td>Supported on IB-FLEX platforms, but you cannot enable Software ADP and DNS cache acceleration simultaneously.</td>
</tr>
</tbody>
</table>

**Viewing Accelerated Cache Details**

When you view cached contents of the DNS accelerator through the Grid Manager, there might be a slight impact on the DNS query performance of the selected member.

To view accelerated cache from the Grid Manager:

1. From the Data Management tab, select the DNS tab and click the Members tab -> member check box. Choose View from the Toolbar, and click View Cache.
2. Click Yes in the View Acceleration Cache dialog box.
3. The system displays a File Download was Successful message and the cache data is displayed in table format in a new browser tab or browser window.
Limitations for Virtual DNS Cache Acceleration

- You cannot enable the DNS cache acceleration feature during a scheduled NIOS upgrade, but if you have already enabled this feature, then it will function normally during the upgrade process.
- The appliance prompts for a reboot when you enable the DNS cache acceleration feature for the first time. You must accept it to start the service.
- Infoblox does not support enabling the Software ADP and DNS cache acceleration features simultaneously on IB-FLEX.
- You must disable the DNS cache acceleration feature and reboot the appliance manually to switch from virtual DNS cache acceleration to authoritative servers.
- The appliance prompts for a reboot when you disable virtual DNS cache acceleration and enable Software ADP and vice versa.

IB-FLEX Platform Settings for DNS Cache Acceleration

When you enable the DNS cache acceleration feature on IB-FLEX, ensure that it has enough CPU and memory to start the service, and it does not contain any authoritative zones. Note that you cannot start the service, if the total CPU is less than 8 cores or memory is less than 12G. To start the service, the number of resources mentioned in Table 8.8 are mandatory.

Reports for IB-FLEX

Infoblox supports a selected set of reports on IB-FLEX. To view all available reports, from the Reporting tab, select the Dashboards tab. The table below lists all the supported reports for IB-FLEX. For information about how to create and manage user-defined reports, see Infoblox Reporting and Analytics.

Table 9 Supported Reports for IB-FLEX

<table>
<thead>
<tr>
<th>DNS Reports</th>
<th>Security (DNS) Reports</th>
<th>System Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Query Rate by Query Type</td>
<td>DNS Top RPZ Hits</td>
<td>Flex Grid Licensing Features Enabled</td>
</tr>
<tr>
<td>DNS Query Rate by Member</td>
<td>DNS Top RPZ Hits by Client</td>
<td>CPU Utilization Trend</td>
</tr>
<tr>
<td>DNS Daily Query Rate by Member</td>
<td>DNS RPZ Hits Trend By Mitigation Action</td>
<td>Memory Utilization Trend</td>
</tr>
<tr>
<td>DNS Daily Peak Hour Query Rate by Member</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Replies Trend</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Cache Hit Rate Trend</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top Requested Domain Names</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top NXDOMAIN / NOERROR (no data)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top Clients</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top Timed-Out Recursive Queries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Response Latency Trend</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top SERVFAIL Errors Sent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top SERVFAIL Errors Received</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Object Count Trend for Flex Grid License</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Effective Peak Usage Trend for Flex Grid License</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

About Elastic Scaling

Elastic Scaling provides the capability to automatically pre-provision and deploy vNIOS appliances on-demand for IPAM (IP Address Management), DNS, and/or DHCP. Compared to standard appliance deployment and licensing management, you now have the flexibility to purchase multiple service and feature licenses and install them as dynamic licenses for future vNIOS or cloud deployments based on your evolving business needs and deploy them as needed. When you remove a vNIOS or cloud appliance from the Grid, the dynamic licenses on the appliance are automatically released and returned to the license pool on the Grid Master for reuse at a later time. Elastic scaling includes a full set
of APIs for pre-provisioning, deployment, and de-provisioning vNIOS appliances, making it simple to add or remove DNS or DHCP capacity on-demand to meet changing infrastructure requirements. This is critical for realizing the benefits of dynamic Cloud environments. For information about the Infoblox cloud solution, see Deploying Cloud Network Automation.

You can purchase licenses of any type, such as vNIOS, DNS, DHCP, Enterprise (formerly Grid) and Cloud Platform, deploy them as dynamic licenses on the Grid Master, and allocate them to vNIOS virtual appliances manually or automatically through Elastic Scaling.

All dynamic licenses are tied to a specific Grid Master. You must first obtain the LPC_UID (License Pool Container Unique ID) of the Grid Master before obtaining the licenses from Infoblox Technical Support. For more information, see Obtaining Dynamic Licenses.

When you use Elastic Scaling to pre-provision and launch vNIOS appliances, licenses are automatically installed on the newly spun-up appliances during the process as long as you have the correct vNIOS licenses in the license pools for the vNIOS models you plan to deploy. For example, you can install a CP-V1400 license on a CP-V1400 or CP-V800, but you cannot do so on a CP-V2200. If there are no licenses available in the pool for the specified appliance models, the Grid Master notifies you with an error message (for Cloud Platform Appliances, the API calls fail). Note that you cannot add a vNIOS Grid member when no dynamic licenses are available. When you spin down vNIOS appliances, its assigned licenses are released and returned to the NIOS license pool.

The Grid Master keeps track of dynamic licenses that are allocated to vNIOS members and adjusts the total number of available dynamic licenses for each feature and service. You can view the total number of dynamic licenses installed for each feature and service, the number of active and available licenses, their usage, and other related information in the Grid tab -> Licenses tab -> Pool tab of Grid Manager. For information about how to view dynamic licenses, see Viewing Dynamic Licenses.

Infoblox supports elastic scaling for Software ADP profiles on the supported platforms and provides the following pool licenses: Threat Protection (Software add-on) and Threat Protection Update. For more information about Software ADP profiles, see Configuring Threat Protection Profiles. Threat protection members use management port for IPv4 and IPv6 communication with the Grid. Infoblox supports cloud API calls for such members to join the Grid using MGMT port and VPN on the MGMT port. To know more about using the MGMT port, see Using the MGMT Port. You can also manually allocate and deallocate dynamic licenses as your business requirements evolve. For more information, see Manually Allocating Dynamic Licenses and Manually Deallocating Dynamic Licenses.

### Using Elastic Scaling to Pre-provision and Launch vNIOS Members

You can use Elastic Scaling to deploy on-demand vNIOS virtual members in a Grid and in your cloud environment and pre-provision them to manage networks and zones. For information about how to utilize Elastic Scaling to provision Cloud Platform Appliances and join them to the Grid using cloud API calls, see Sample Cloud API Requests for Elastic Scaling.

The following tasks to pre-provision and launch vNIOS appliances:

1. Obtain dynamic licenses and install them on the Grid Master, as described in Obtaining Dynamic Licenses. You can also use a temporary license to spin up a Grid Master VM.
2. Create an offline Grid member or HA pair, as described in Adding a Single Member or Adding an HA Member.
3. Pre-provision the offline Grid member you just created, as described in Configuring Pre-Provisioned Members. Note that there are a few guidelines that you might want to review before pre-provisioning your Grid member. For more information, see Guidelines for Pre-provisioning Offline Grid Members.

   **Note:** You must include the Grid and vNIOS provisional licenses for pre-provisioned vNIOS members in order to join them to the Grid.

4. Generate a token for the Grid member, as described in Generating Tokens for Grid Members.

   **Note:** For HA pairs, the appliance generates two tokens—one for each node of the HA pair.

5. Use cloud API calls to add network views, networks, or zones and then delegate the objects to the offline Grid member. For information about sample cloud API requests, see Sample Cloud API Requests for Elastic Scaling.
6. Use API requests to join the Grid member to the Grid. For sample API requests, see Sample Cloud API Requests for Elastic Scaling. If for any reasons the automated process of Elastic Scaling fails or if you are unable to send API calls, you can use CLI commands to join the Grid member to the Grid as a workaround. For more information, see Using CLI Commands to Join Grid Members.
7. Verify the Grid member has successfully joined the Grid, as described in Viewing Status.
8. Verify the dynamic licenses have been allocated correctly by viewing the license usage, as described in Viewing Dynamic Licenses.

### Generating Tokens for Grid Members

Before you can automatically allocate dynamic licenses to a pre-provisioned member, you must request a one-time token from the Grid Master. This token allows the member to register and authenticate itself to the Grid Master before a specified date and time (the default is 60 minutes from the time you generate the token). When the token is not used after the expiration date and time, it becomes invalid and you must generate another token for the member. You can configure the token usage timeout so the appliance can send syslog messages to alert you about the unused token. For information about how to set the token usage timeout value, see Configuring Token Usage Timeout.

Using a one-time token eliminates the need for the Grid Master credentials to be exposed to other Grid members and the CMP (Cloud Management Platform) in the case of cloud implementation. Note that only superusers can generate and view the token for a pre-provisioned Grid member.

**Note:** You can use API calls as part of the automated deployment process to generate a token for the vNIOS Grid member before joining it to the Grid. For information about sample API requests you can use to generate a token, see Sample Cloud API Requests for Elastic Scaling. As a workaround, you can also generate a token through Grid Manager.

To generate a token through Grid Manager, complete the following:
1. From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab.

2. Click the **Action** icon (shown as a gear in each row for the table) next to the vNIOS member and select **Generate Token** from the list.

3. In the **Your Permission Token** dialog, the appliance displays the token and the **Expiration Date** of the token. You must generate a new token for the member if the token is not used before the expiration date.

   **Note:** Copy this token and paste it at the CLI when you use the set token on command to set the token and generate the token file.

### Configuring Token Usage Timeout

You can configure the appliance to send syslog messages to alert you about an unused token that has been generated for a pre-provisioned member. Depending on the timeout interval you configure, the appliance sends a syslog message for each timeout interval until the token expires.

To configure the token usage timeout value:

1. From the **Grid** tab -> **Grid Manager** tab, click **Grid Properties** -> **Edit** from the toolbar.
2. In the **Grid Properties** editor, select the **General** tab -> **Basic** tab and complete the following:
   - **Token usage timeout:** Enter the time interval (in minutes) for which the appliance sends a syslog message to alert you about the unused permission token for a pre-provisioned member. For example, if you enter 5 here, the appliance sends a syslog message every five minutes. The default is 10.
3. Save the configuration.

### Using CLI Commands to Join Grid Members

**Note:** If for any reasons the automated process of Elastic Scaling does not function properly, you can use CLI commands to join Grid members to the Grid as a workaround.

When using Elastic Scaling, ensure that you have generated a token for the member, as described in **Generating Tokens for Grid Members** before joining the member to the Grid.

To join the vNIOS member to the Grid:

1. Access the Infoblox CLI using an SSHv2 connection through an SSHv2 client. You can also access the CLI by connecting a serial cable directly from the console port of a management system to the console port on the appliance, and then using a terminal emulation program such as Hilgraeve Hyperterminal® (provided with Windows® operating systems) and launch a session. The connection settings are:
   - Bits per second: 9600
   - Stop bits: 1
   - Data bits: 8
   - Flow control: Xon/Xoff
   - Parity: None

2. Log in using the default user name and password **admin** and **infoblox**. User names and passwords are case-sensitive.
3. To change the network settings from the default, enter the **set network** command. Then enter information as prompted to change the IP address, netmask, and gateway for the LAN1 port.

   ```
   Infoblox > set network
   NOTICE: All HA configuration is performed from the GUI. This interface is used only to configure a standalone node or to join a grid.
   Enter IPv4 address [Default: n.n.n.41]: <Enter the LAN1 port IP address>
   Enter netmask [Default: 255.255.255.0]: <Enter the LAN1 port netmask>
   Enter gateway address [Default: n.n.n.1]: <Enter the gateway IP address>
   NOTICE: Additional IPv6 interface can be configured only via GUI.
   Become grid member? (y or n): n
   ```

   **Note:** You must enter **n** to use Elastic Scaling. If you enter **y**, the member becomes a Grid member and you will not be able to set token and join the pre-provisioned member to the Grid.

4. Use the **set token on** command to set the member token, the Grid Master IP address and certificate to the token file. Following is an example:

   ```
   Infoblox > set token on
   Enter GM-IP [Current: not defined]: <Enter the Grid Master IP address>
   Enter Token [Current: not defined]: Copy token from the Your Permission Token dialog in Grid Manager.
   New Token Settings:
   GM-IP: 1.1.1.1
   Token: b251lnZpcnR1YWxfhm9KZSQx
   Is this correct? (y or n): y
   Do you want to download the certificate form GM and validate (y or n): y
   Is this correct and valid (y or n): y
   ```
4. Are you sure to apply and save settings to file?: y
   The token and certificate are saved.
5. To verify the token:
   Infoblox > show token
   The CLI displays the current token setting and certification information. Verify this information.

   **Note:** If there is incorrect information, use set token off to remove the token file.
6. Use the set token join command to register the Grid member and get licenses from the license pool before joining the member to the Grid. Once the member joins the Grid, the token become invalid—you can use the token only once.
   Infoblox > set token join
   Are you sure to start Member registration Client? (y or no): y Starting Member registration Client...
   Connecting...

   **Note:** For HA pairs, repeat the CLI commands on both nodes.

Using OpenStack cloud-init template to configure Grid Master and join Grid members

You can use the following OpenStack cloud-init template to configure an IB-V815 as a Grid Master:

```
#infoblox-config remote_console_enabled: y default_admin_password: infoblox
temp_license: nios IB-V815 dns dhcp enterprise
lan1:
  v4_addr: 10.2.0.132
  v4_netmask: 255.255.255.0
  v4_gw: 10.2.0.1
mgmt:
  v4_addr: 10.1.0.69
  v4_netmask: 255.255.255.0
  v4_gw: 10.1.0.1
```

You can use the following OpenStack cloud-init template to join an IB-V815 member to the Grid:

```
#infoblox-config remote_console_enabled: y default_admin_password: infoblox
temp_license: nios IB-V815 dns dhcp enterprise sw_tp tp_sub lan1:
  v4_addr: 10.2.0.140
  v4_netmask: 255.255.255.0
  v4_gw: 10.2.0.1
mgmt:
  v4_addr: 10.1.0.77
  v4_netmask: 255.255.255.0
  v4_gw: 10.1.0.1
gridmaster:
  token: xqyv+gEcPlIUp9ETDhqmS2VcFiHEd81/U ip_addr: 10.39.8.109
  join_intf: mgmt
certificate: -----BEGIN CERTIFICATE-----MIIDdzCCAl8CEBgaZIhvcNCAQEFBQAwejELMAkGA1UEBhMCVVMx
```
You can use the following OpenStack cloud-init template to join an IB-V1415 member to the Grid:

```
#infoblox-config remote_console_enabled: y default_admin_password: infoblox
temp_license: nios IB-V1415 dns dhcp enterprise sw_tp tp_sub
#temp_license: nios IB-FLEX

lan1:

  v4_addr: 10.2.0.28
  v4_netmask: 255.255.255.0
  v4_gw: 10.2.0.1

ha:

  v4_addr: 10.2.0.30
  v4_netmask: 255.255.255.0
  v4_gw: 10.2.0.1

mgmt:

  v4_addr: 10.1.0.29
  v4_netmask: 255.255.255.0
  v4_gw: 10.1.0.1

gridmaster:

token: 0rPidqD1Iau91adaIL7zlO7sZb0qxuk1 ip_addr: 10.39.52.19
join_intf: mgmt

certificate: -----BEGIN CERTIFICATE-----

You can use the following OpenStack cloud-init template to join an IB-V825 member to the Grid:

```
#infoblox-config remote_console_enabled: y default_admin_password: infoblox
temp_license: nios IB-V825 dns dhcp enterprise

lan1:

  v6_addr: 2620:10a:6000:2708::17
  v6_cidr: 64
  v6_gw: 2620:10a:6000:2708::1

mgmt:

  v6_addr: 2620:10a:6000:2701::a
  v6_cidr: 64
  v6_gw: 2620:10a:6000:2701::1
```
gridmaster:

token: IDuxCCzc/o08PHUURVVTGKoEUSq0x0 ip_addr: 2620:10a:6000:2701::8
join_intf: mgmt
certificate: -----BEGIN CERTIFICATE-----MIIDdzCCAl8CEDdxmmxPWbgZpPZFy0lfzowDQYJKoZIhvcNAQEFBQAwjeElMAkGA1UEBhMCVVMxCzA8CEDdxmmxPWbgZpPZFy0lfzowDQYJKoZIhvcNAQEFBQAwjeElMAkGA1UEBhMCVVMxCzA8CEDdxmmxPWbgZpPZFy0lfzow
gridactivation:

#infoblox-config remote_console_enabled: y
default_admin_password: infoblox hardware_type: IB-FLEX temp_license: flex grid activation

lan1:
v4_addr: 255.255.255.0
v4_netmask: 255.255.255.0
v4_gw: 10.1.0.1
mgmt:
v4_addr: 255.255.255.0
v4_netmask: 255.255.255.0
v4_gw: 10.1.0.1

Managing the Order of Match Lists

When you configure certain DNS and DHCP functions, you can create match lists that the appliance uses to filter specific IP addresses for specific operations. For example, you can create a DNS blackhole list for including and excluding DNS traffic to certain IP addresses, configure a list of IP addresses for allowing and denying DDNS updates, or define a Match Destinations list that identifies destination addresses and TSIG keys that are allowed access to a DNS view.

The appliance matches rules in these lists from top to bottom. Rules at the top always take precedence over those at the bottom. Therefore, ensure that you put the most specific rules at the top of the list, and then put the more general rules at the bottom. For example, when you add network 10.10.0.0/24 to a DNS blackhole list, all 256 IP addresses in the network are put on the blackhole list. To allow DNS traffic to the specific IP addresses 10.10.0.55 and 10.10.0.88, you must add these two addresses at the top of the blackhole list before the network address 10.10.0.0/24, and then set their permissions to "Exclude." The same applies when you set up the list of clients for DDNS updates. If you want to deny DDNS updates from a specific client (10.0.0.99) and allow DDNS updates from all other clients in the 10.0.0.0/24 network, you must put 10.0.0.99 at the top of the list and configure the appliance to deny DDNS updates from this client. You then add network 10.0.0.0/24 for allowing DDNS updates from all other clients at the bottom of the list.

Managing NIOS Appliances

To reboot and shut down a NIOS appliance, you can use Grid Manager or the Infoblox CLI. To reset a NIOS appliance, you must use the Infoblox CLI. You can also restart a Grid member or restart a GUI session through Grid Manager. You can also force an HA failover using the GUI.

Restarting a Grid Member

You can restart a single Grid member or an HA pair on the NIOS appliance. When you restart a Grid member, the appliance logs the task in the audit log.

To restart a single Grid member:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box.
2. Expand the Toolbar and click Control -> Restart.
3. In the Restart on Product dialog box, click OK to restart the Grid member.

Rebooting a NIOS Appliance
You can reboot a single NIOS appliance, a single node in an HA pair, or both nodes in an HA pair. To reboot a single NIOS appliance or one or both nodes in an HA pair:

1. From the **Grid** tab, select the **GridManager** tab -> **Members** tab -> **Grid_member** check box.
2. Expand the Toolbar and click **Control** -> **Reboot**.
   - For an HA pair, choose whether to reboot one node (and which one) or both nodes, and then click **OK**. Depending on the browser you use, Grid Manager may display a dialog box that indicates the system is unavailable during a restart or reboot.

To reboot a single NIOS appliance using the CLI:

1. Log in to the Infoblox CLI using a superuser account for the NIOS appliance that you intend to reboot.
2. Enter the following CLI command: `reboot`

**Shutting Down a NIOS Appliance**

Under normal circumstances, you do not need to turn off or shut down a NIOS appliance. It is designed to operate continuously. However, if you want to turn off a NIOS appliance, use the GUI or the CLI to shut down the appliance, instead of just turning off the power switch.

**Note:** If there is a disruption in power when the NIOS appliance is operating, the NIOS appliance automatically reboots itself when power is restored.

To shut down a NIOS appliance:

1. From the **Grid** tab, select the **GridManager** tab -> **Members** tab -> **Grid_member** check box.
2. Expand the Toolbar and click **Control** -> **Shutdown**.
   - For an HA pair, choose whether to shut down one node (and which one) or both nodes, and then click **OK**. The NIOS appliance shuts down. The fans might continue to operate until the appliance cools down.

To shut down a NIOS appliance using the CLI:

1. Log in to the Infoblox CLI using a superuser account.
2. Enter the following CLI command: `shutdown`

**Forcing an HA Failover**

If you want to change which node in an HA pair is active and which is passive, you can force a failover to occur. Within five seconds after initiating a failover, the previously passive node becomes active and assumes ownership of the VIP address. Note that a forced failover causes a temporary service disruption. To proceed with the forced failover, click **OK**. The appliance logs this task in the audit log.

To restart a single Grid member:

1. From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **Grid_member** check box.

   **Note:** The Grid member that you select must be an HA pair.

2. Expand the Toolbar and click **Control** -> **Force HA Failover**.
3. In the **For HA Failover** dialog box, click **OK** to change the node in an HA pair.

**Restarting GUI Sessions**

You can restart a GUI session through Grid Manager. When you restart GUI on a specific member, the appliance logs off all other GUI sessions that are currently running even though they are opened in different browsers or another system. The appliance logs this task in the audit log.

To restart GUI sessions on a Grid member:

1. From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **Grid_member** check box.
2. Expand the Toolbar and click **Control** -> **Restart GUI**.
3. In the **Restart GUI** dialog box, click **OK** to restart the NIOS appliance.

**Resetting a NIOS Appliance**

There are three ways to reset a NIOS appliance:

- **Resetting the Database**
- **Resetting a NIOS Appliance to Factory Settings**
Resetting the NIOS Appliance to Factory Settings and Removing Licenses You can perform these functions only through the CLI.

Resetting the Database
You can reset the database if you lose the administrator account and password or if you want to clear the database but preserve the log files to diagnose a problem. This function removes the configuration files, and the DNS and DHCP data from the appliance database. During this procedure, you are given the option to preserve the network settings of the appliance, which are the IP address and subnet mask, the IP address of the gateway, the host name, and the remote access setting.

To reset the database:
1. Log in to the Infoblox CLI using a superuser account.
2. Enter the following CLI command: `reset database`
   The appliance then displays a message similar to the following:
   The following network settings can be restored after reset: IP Address: 10.1.1.10
   Subnet Mask: 255.255.255.0
   Gateway: 10.1.1.1
   Host Name: ns1.corpxyz.com Remote Console Access: true
   The entire database will be erased.
   Do you wish to preserve basic network settings? (y or n)
   Press the Y key to preserve the network settings or the N key to return the network settings to their default values (192.168.1.2, 255.255.255.0, 192.168.1.1).

Resetting a NIOS Appliance to Factory Settings

You can reset a NIOS appliance to its original factory settings. This removes the database, network settings, logs, and configuration files. Then, it reboots with its factory settings, which are the default user name and password, and default network settings. When you perform this procedure, the appliance does not give you the option to preserve your network settings.

Note: If you have previously imported HTTPS certificates, the appliance regenerates the certificates and replaces them.

To reset the NIOS appliance to its factory settings:
1. Log in to the Infoblox CLI using a superuser account.
2. Enter the following CLI command: `reset all`

Resetting the NIOS Appliance to Factory Settings and Removing Licenses

You can also reset a NIOS appliance to its original factory settings and remove all the licenses installed on the appliance. This removes the database, network settings, logs, configuration files, and licenses. The appliance then reboots with its factory settings, which are the default user name and password, and default network settings.

Note: If you have previously imported HTTPS certificates, the NIOS appliance regenerates the certificates and replaces them.

To reset the NIOS appliance to its factory settings and remove all its licenses:
1. Log in to the Infoblox CLI using a superuser account.
2. Enter the following CLI command: `reset all licenses`.

Managing the Disk Subsystem on the Infoblox-4010

Among its many features, the Infoblox-4010 use a RAID (Redundant Array of Independent Disks) 10 array to provide the optimum mix of high database performance and redundant data storage with recovery features in the event of disk failures. The disk array is completely self managed. There are no maintenance or special procedures required to service the disk subsystem.

Caution: Never remove more than one disk at a time from the array. Removing two or more disks at once can cause an array failure and result in an unrecoverable condition. You should replace only one disk at a time, using a replacement disk from Infoblox. For information, see Replacing a Failed Disk Drive.

About RAID 10

RAID 10 (or sometimes called RAID 1+0) uses a minimum of four disk drives to create a RAID 0 array from two RAID 1 arrays, as shown in Figure 8.15. It uses mirroring and striping to form a stripe of mirrored subsets. This means that the array combines—or stripes—multiple disk drives, creating a single logical volume (RAID 0). RAID 10 combines the high performance of RAID 0 and the high fault tolerance of RAID 1. Striping disk drives improves database write performance over a single disk drive for large databases. The disks are also mirrored (RAID 1), so that each disk in the logical volume is fully redundant.

Figure 8.15 RAID 10 Array Configuration
Evaluating the Status of the Disk Subsystem

You can monitor the disk subsystem through the Infoblox Grid Manager GUI, the scrolling front panel LCD display, and four front panel LEDs next to the disk drives. In addition, you can monitor the disk status by using the CLI command `show hardware_status`. The following example displays the status of an Infoblox-4010 using the command:

```
Infoblox > show hardware_status
```

```
POWER: Power OK
Fan1: 7258 RPM
Fan2: 6887 RPM
Fan3: 7258 RPM
CPU1_TEMP: +20.0 C
CPU2_TEMP: +24.0 C
SYS_TEMP: +35 C
```

The panel provides a detailed status report on the appliance and service operations. To see a detailed status report:

- From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box -> Detailed Status icon in the table toolbar.

After displaying the Detailed Status panel, you can view the status of the selected Grid member. For more information on the Detailed Status panel, see Viewing Status.

The RAID icons indicate the status of the RAID array on the Infoblox-4010.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The RAID array is in an optimal state.</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>A new disk was inserted and the RAID array is rebuilding.</td>
<td></td>
</tr>
<tr>
<td>Red</td>
<td>The RAID array is degraded. At least one disk is not functioning properly. The GUI lists the disks that are online. Replace only the disks that are offline.</td>
<td></td>
</tr>
</tbody>
</table>

The appliance also displays the type of each disk. In the event of a disk failure, you must replace the failed disk with one that is qualified and shipped from Infoblox and has the same disk type as the rest of the disks in the array.

Infoblox-4010 uses only the IB-Type 3 disk type. All disk drives in the array must have the same disk type for the array to function properly. You can have either IB-Type 1, IB-Type 2, or IB-Type-3, but you cannot mix both in the array. When you have a mismatched disk in the array, you must promptly replace the disk with a replacement disk from Infoblox to avoid operational issues.
Disk Drive Front Panel LEDs

The disk drives of the Infoblox-4010 are located on the appliance front panel. To the right of each drive, two LEDs display connection and activity status. Table 8.10 lists the disk drive LED combinations and the states they represent.

Table 8.10 Infoblox-4010 Disk Drive LED Combinations

<table>
<thead>
<tr>
<th>Online/Activity LED (Green)</th>
<th>Fault/UID LED (Amber/Blue)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On, off, or blinking</td>
<td>Alternating amber and blue</td>
<td>The drive has failed, or it has received a predictive failure alert; it also has been selected by a management application.</td>
</tr>
<tr>
<td>On, off, or blinking</td>
<td>Steadily blue</td>
<td>The drive is operating normally.</td>
</tr>
<tr>
<td>On</td>
<td>Amber, blinking regularly (1 Hz)</td>
<td>The drive has received a predictive failure alert. Replace the drive as soon as possible.</td>
</tr>
<tr>
<td>Blinking regularly (1Hz)</td>
<td>Off</td>
<td>Do not remove the drive. The drive is rebuilding. Removing the drive may terminate the current operation and cause data loss.</td>
</tr>
<tr>
<td>Blinking irregularly</td>
<td>Amber, blinking regularly (1 Hz)</td>
<td>The drive is active, but it has received a predictive failure alert. Replace the drive as soon as possible.</td>
</tr>
<tr>
<td>Blinking irregularly</td>
<td>Off</td>
<td>The drive is active and operating normally.</td>
</tr>
<tr>
<td>Off</td>
<td>Steadily amber</td>
<td>A critical fault condition has been identified for this drive, and the controller has placed it offline. Replace the drive as soon as possible.</td>
</tr>
<tr>
<td>Off</td>
<td>Amber, blinking regularly (1 Hz)</td>
<td>The drive has received a predictive failure alert. Replace the drive as soon as possible.</td>
</tr>
<tr>
<td>Off</td>
<td>Off</td>
<td>The drive is offline, a spare, or not configured as part of an array.</td>
</tr>
</tbody>
</table>

Replacing a Failed Disk Drive

The Infoblox-4010 is designed to provide continuous operation in the event of a failed disk. Replace an original RAID disk only when there is a disk failure. Hot-swapping a disk drive is a simple process that does not require issuing commands or a GUI operation.

When you replace a failed disk, you must replace it with an Infoblox supplied disk. To ensure that you receive the correct replacement disk, report the disk type or part number of the failed disk. The appliance displays the disk type in the Detailed Status panel, and the Infoblox part number is printed on the disk. Installing disks that are not qualified and shipped from Infoblox could cause failures in the appliance.

To replace a disk drive, follow this procedure:

1. Identify and verify the failed drive via the Grid Manager, front panel LCD, or CLI. Make sure you have identified the correct drive.
2. Insert the replacement drive into the drive bay slot.
3. Gently slide the drive into place. When you feel the release lever engage, continue applying gentle pressure to the drive while pushing the release lever towards the appliance.
4. The release lever locks into place and the LED next to the disk drive lights up. Note that if the alarm buzzer is sounding, it automatically turns off about 20 seconds after the drive is inserted.
5. The disk drive automatically goes into rebuild mode.

Disk Array Guidelines

Infoblox has designed the disk array to be completely self managed. There are no maintenance procedures required for a normally functioning disk array. Mishandling the disk array can cause an unrecoverable error and result in a failed appliance. Infoblox highly recommends that you...
When you make configuration changes for DNS or DHCP and the service is enabled on at least one Grid member, Grid Manager suggests a service restart. You can enable the service restart banner by clicking the Restart Banner button. Whenever you make a change such as adding a zone or a network, Grid Manager notifies you that a service restart is required. You can enable the appliance to display the Restart Banner whenever it requires a service restart and prompt the administrator to input the user name before restarting the services. For information about how to enable the restart banner, see Changing Grid Properties. To view all pending activities that are waiting for service restart, you can click View Changes in the restart banner at the top of Grid Manager.

The pending activities include additions, modifications, and deletions performed by all administrators. You can also view pending changes through the Restart Grid/Member Services dialog box.

There are several ways to restart services on the affected Grid members. You can restart services at the Grid or member level, or you can restart services by groups, as described in:

- Restarting Grid Services
- Restarting Member Services
- Restarting Services by Groups

You can configure services restart settings such as restart timeout or delay as described in Configuring Restart Settings.

**Note:** When you make configuration changes for DNS or DHCP and the service is enabled on at least one Grid member, Grid Manager suggests a restart even if the service is disabled on the member affected by the change.

### User Permissions for Restarting Services

The following rules apply to superusers and limited-access users:

- You can cancel a schedule task that you create to restart a service. A superuser can cancel any scheduled restart task.
- Only superusers and administrators with read/write permission to all Grid members can schedule a Grid restart task.
- When a superuser schedules a Grid restart task, a limited-access user cannot schedule a member-level restart task.
- Limited-access users cannot cancel a superuser's scheduled tasks.
- Limited-access users cannot create or modify a scheduled restart task for a Grid member if a scheduled restart task for the member (created by another user) already exists.

The system writes every scheduled change action to the audit log as follows:

```plaintext
USER logon_id action service restart schedule 'schedule' on Grid (or member) Grid name or member node id
```

For example:

```plaintext
USER jdoe insert service restart schedule '02/20/2007 01:30:00' on Grid Infoblox USER jdoe deleted service restart schedule '02/22/2007 01:30:00' on node id 3
```

### Restarting Services

Whenever you make a change such as adding a zone or a network, Grid Manager notifies you that a service restart is required. You can enable the appliance to display the Restart Banner whenever it requires a service restart and prompt the administrator to input the user name before restarting the services. For information about how to enable the restart banner, see Changing Grid Properties. To view all pending activities that are waiting for service restart, you can click View Changes in the restart banner at the top of Grid Manager.

The pending activities include additions, modifications, and deletions performed by all administrators. You can also view pending changes through the Restart Grid/Member Services dialog box.

There are several ways to restart services on the affected Grid members. You can restart services at the Grid or member level, or you can restart services by groups, as described in:

- Restarting Grid Services
- Restarting Member Services
- Restarting Services by Groups

You can configure services restart settings such as restart timeout or delay as described in Configuring Restart Settings.

### User Permissions for Restarting Services

The following rules apply to superusers and limited-access users:

- You can cancel a schedule task that you create to restart a service. A superuser can cancel any scheduled restart task.
- Only superusers and administrators with read/write permission to all Grid members can schedule a Grid restart task.
- When a superuser schedules a Grid restart task, a limited-access user cannot schedule a member-level restart task.
- Limited-access users cannot cancel a superuser's scheduled tasks.
- Limited-access users cannot create or modify a scheduled restart task for a Grid member if a scheduled restart task for the member (created by another user) already exists.

The system writes every scheduled change action to the audit log as follows:

```plaintext
USER logon_id action service restart schedule 'schedule' on Grid (or member) Grid name or member node id
```

For example:

```plaintext
USER jdoe insert service restart schedule '02/20/2007 01:30:00' on Grid Infoblox USER jdoe deleted service restart schedule '02/22/2007 01:30:00' on node id 3
```
For more information on the audit log, see Using the Audit Log.

Restarting Grid Services

Only superusers and administrators with read/write permission to all Grid members can schedule a Grid restart task. You can restart services at the Grid level either simultaneously or sequentially, and can also specify the restart time. If you schedule the restart at a specific date and time, the system schedules the restart at the specified time on each Grid member.

To restart services at the Grid level:

1. From the Data Management tab, select the DHCP, DNS, or Grid tab, or select the Administration tab, and then click Restart Services from the Toolbar.

The Restart Grid Services dialog appears.

1. You can specify whether the member restarts services when necessary or you can force it to restart services. Select one of the following in the Restart Grid Services section:
   - If needed: Select this to restart all active DNS and DHCP services if there are any changes requiring a service restart.
   - Force service restart: Select this to force a service restart even if it is not needed. A forced restart may be delayed if there are pending restarts for the same service.

2. Select one of the following in the Restart Method section:
   - Restart All Restart Groups: Restarts the services in the affected Grid members in the order defined for restart groups. For information, see Restarting Grid Services.
   - Simultaneously for all members: Restarts the services on all of the members in a Grid at the same time.
   - Sequentially for all members: Restarts the services on each Grid member one after one. If this option is selected, once a member restarts services, the administrator can select to restart services in the other Grid members in sequential order.
   - Affected Members and Services: Click the Poll Members icon to display the affected members and services when the system restarts. Grid Manager displays the member names and one of the following for each service:
     - YES: The service is active and the system will restart the service upon execution of this task.
     - NO: The service will not restart unless the Force service restart option is selected.
     - DISABLED: The service is currently disabled.

View Pending Changes: You can view the list of pending changes that will take effect when you restart the services. You can use filters to look for specific objects and view the following information for each pending activity:

- Timestamp: The timestamp of the operation.
- Admin: The admin user who performed the operation.
- Action: The type of operation that was performed by an administrator. This can be Created, Modified, Deleted, Called, or Messages.
- Object Type: Displays the object type. For example, DNS View, Named ACL, IPv4 MAC Filter, Blacklist Rule, and so on.
- Object Name: The name of the object.
- Message: Description of the activity.

3. To schedule a service restart task, click the Schedule icon at the top of the wizard. In the Schedule Change panel, complete the following:
   - Now: Restarts services upon clicking Restart.
   - Later: Enter the following information to schedule all Grid members to restart services at a certain date and time:
     - Date: Enter a date in YYYY-MM-DD (year-month-day) format. The appliance displays today's date. You can also click the calendar icon to select a date from the calendar widget.
     - Time: Enter a time in h:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. When you enter the time in a 24-hour format such as 23:00, Grid Manager displays 11:00:00 PM. You can also select a time from the drop-down list by clicking the time icon.
     - Time Zone: Select a time zone for the scheduled date and time from the drop-down list. This field displays the time zone of the browser that the admin uses to log in to Grid Manager.

4. Click Restart to restart services immediately or click Schedule Restart to create a scheduled restart task.

Note: When you restart services at the Grid level, the services are restarted only on those members for which you have permissions.

Restarting Member Services

The member restart time always supersedes the Grid restart time. If the member restart time is later than the Grid restart time, then the member restarts services at its scheduled time. If the member restart time is before the Grid restart time, then the member restarts services at the member's scheduled restart time, and again during the Grid restart time.

To restart member services:

1. From the Data Management tab, select the DHCP tab -> Members tab -> member check box.
   or
   From the Grid tab, select the Grid Manager tab, and then select a member check box.
2. Click Restart Services from the Toolbar.
3. You can specify whether the member should restart services when necessary or you can force it to restart services. Select one of the following in the Restart Member Services section:
   - If needed: Select this to restart all active DNS and DHCP services, if there are any changes requiring a service restart.
   - Force service restart: Select this to force a service restart even if it is not needed. A forced restart may be delayed if there are
pending restarts for the same service.

**Affected Services**: This table displays the affected services when the system restarts. It can display one of the following for each service:
- **YES**: The service is active and the system will restart the service upon execution of this task.
- **NO**: The service will not restart unless the **Force service restart** option is selected.
- **DISABLED**: The service is currently disabled.

**View Pending Changes**: You can view the list of pending changes that will take effect when you restart the services. You can use filters to look for specific objects and view the following information for each pending activity:
- **Timestamp**: The timestamp of the operation.
- **Admin**: The admin user who performed the operation.
- **Action**: The type of operation that was performed by an administrator. This can be **Created**, **Modified**, **Deleted**, **Called**, or **Message**.
- **Object Type**: Displays the object type. For example, DNS View, Named ACL, IPv4 MAC Filter, Blacklist Rule, and so on.
- **Object Name**: The name of the object.
- **Message**: Description of the activity.

4. To schedule a service restart task, click the Schedule icon at the top of the editor. In the **Schedule Change** panel, complete the following:
- **Now**: Restarts services immediately.
- **Later**: Enter the following information to schedule the member to restart services at a certain date and time:
  - **Date**: Enter a date in YYYY-MM-DD (year-month-day) format. The appliance displays today's date. You can also click the calendar icon to select a date from the calendar widget.
  - **Time**: Enter a time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.
  - **Time Zone**: Select a time zone for the scheduled date and time from the drop-down list. This field displays the time zone of the browser that the admin uses to log in to Grid Manager.

5. Click **Restart** to restart services immediately or click **Schedule Restart** to create a scheduled restart task.

### Restarting Services by Groups

You can use the group restart feature for the DHCP and DNS services. You do this by adding Grid members to groups and defining the restart order. Each service has a separate set of groups. You can specify whether a group is restarted sequentially or simultaneously and can also create a recurring schedule for restarts.

To access restart groups:

1. Click **Grid → Grid Manager → DHCP or DNS**.
2. On the **Services** tab, click **Toggle Restart Groups View**.

You can arrange group restart order for each service independently. Members in a group can restart simultaneously or sequentially, depending on your choice. When members are started sequentially, they are started in alphabetical order. When you have several restart groups, they all restart sequentially in the order that you define. For information, see **Ordering Restart Groups**.

For each service, there exists the Default restart group in Grid Manager: Default DHCP group and Default DNS group. All Grid members belong to the Default group until you add them to another custom restart group. By default, the members of the Default group are restarted sequentially. The Default group is always restarted in the last place in the restart sequence for a service.

**Note**: You can manage restart groups only if you are a superuser. If you are a limited-access user, you can see the restart groups and their restart status only if these groups include members for which you have permissions. When you restart services by groups, the services are restarted only on those members for which you have permissions.

For more information on how to create and manage restart groups, see the following sections. For how to restart services by groups, see **Restarting Groups**.

### Creating a Restart Group

You can add a member to a group if the member has a license for the corresponding service. Only members with the appropriate license are available for grouping. For pre-provisioned members, you can add them to groups, but the restart requests are not created for such members.

When you assign members to restart groups, Grid Manager checks if the restart may affect the service operation. If the restart with the current grouping configuration can lead to a service interruption, a warning message is displayed. For example, you cannot add two members from a DHCP failover association to the same group configured to restart its members simultaneously.

To create a restart group:

1. Click **Grid → Grid Manager → DHCP or DNS**.
2. On the **Services** tab, click **Toggle Restart Groups View**.
3. Click the **Add** icon.
4. Specify the general information for the group:
   - Name
   - Comment
   - Restart order for group members: simultaneously or sequentially

**Note**: For how to delay service restarts, see **Configuring Restart Settings**.
5. Click Next.
6. Add members by clicking the Add icon for each new member.
7. Click Next.
8. If you want to create a restart schedule for this group, select Enable Restart Schedule and specify the required parameters.

**Note:** The restart schedule can run either once or on a recurring basis. It does not create scheduled tasks. If a schedule is configured for a restart group, you can still perform one-time restarts independently for Grid members or restart groups and create scheduled tasks for these restarts.

9. Select the restart type for the services on the affected members:
   - If needed: Select this to restart services only if there are changes requiring a service restart.
   - Force service restart: Select this to force a service restart even if it is not needed. A forced restart may be delayed if there are pending restarts for the same service.

10. Click Next.
11. If necessary, specify the extensible attributes.
12. Click Save & Close.

### Editing a Restart Group

You can edit a restart group at any time, even when the restart process is running. The changes do not affect the current restart process.

To edit a restart group:

1. In the restart groups list, select the check box of the group to edit.
2. Click the Edit icon.
3. Edit the group properties as described in **Creating a Restart Group**.
4. Click Save or Save & Close.

### Deleting a Restart Group

You can delete any restart group, except the Default group. When you delete a group, all its members are automatically moved to the Default restart group. You can delete a restart group at any time, even when the restart process is running. The deletion does not affect the current restart process.

To delete a restart group:

1. In the restart groups list, select the check box of the group to delete.
2. Click the Delete icon.

### Ordering Restart Groups

You can modify the order in which multiple groups are restarted. You cannot change the order for the Default group, as it always restarts in the last position by default.

To order restart groups:

1. Go to the restart groups view for the DNS or DHCP service.
2. In the toolbar, click Order Restart Groups.
3. Reorder the groups by using the drag-and-drop operation or by clicking the up and down arrows.
4. Click OK.

### Restarting Groups

When you already have restart groups defined, you can restart services by specific groups at any time after you make configuration changes.

To restart services by groups:

1. Go to the restart groups view for the DNS or DHCP service.
2. Select the groups to restart.
3. In the toolbar, click Restart \(\rightarrow\) Restart Groups.
4. In the Restart Group Confirmation window, select the restart type for the services on the affected members:
   - **If needed**: Select this to restart services only if there are changes requiring a service restart.
   - **Force service restart**: Select this to force a service restart even if it is not needed. A forced restart may be delayed if there are pending restarts for the same service.
5. To schedule a service restart, click the Schedule icon at the top of the wizard. In the **Schedule Change** panel, complete the following:
   - **Now**: Restarts services immediately.
   - **Later**: Enter the following information to schedule the member to restart services at a certain date and time:
     - **Date**: Enter a date in YYYY-MM-DD (year-month-day) format. The appliance displays today's date. You can also click the calendar icon to select a date from the calendar widget.
     - **Time**: Enter a time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.
     - **Time Zone**: Select a time zone for the scheduled date and time from the drop-down list. This field displays the time zone.

5. Optionally, select the check box **Apply restart requests to offline members when they connect.**

6. Click **Save & Close.**

### Chapter 9 File Distribution Services

This chapter describes the file distribution services on the NIOS appliance. It contains the following sections:

- **File Distribution Overview**
- **File Distribution Storage**
  - Usage Threshold Alerts
  - Modifying File Distribution Storage Limits
- **Managing File Distribution Services**
  - Configuring the TFTP Service
  - Configuring the FTP Service
  - Configuring the HTTP Service
  - Configuring Access Control for File Distribution
  - Modifying Access Control Lists
  - Starting and Stopping File Distribution Services
  - Monitoring File Distribution Services
- **Managing Directories**
  - Adding Directories
  - Modifying Directories
  - Creating a Virtual TFTP Root Directory
  - Viewing Directories From the Files Tab
- **Managing Files**
  - Uploading Files
  - Enabling Upload to Grid Members
  - Uploading Files using Grid Manager
  - Uploading Files Using TFTP, FTP, or HTTP File Transfer Client
  - Deleting Files From the Grid Master

---

**Note:** Normally, you cannot restart or schedule a restart of services when a scheduled full Grid upgrade is in progress. However, you can do so for the Default DNS or DHCP restart group. In this case, only the Grid Master is restarted. The other members of the group remain in the Timed Out status and are restarted after Grid Manager gets a response from them. For more information about the full Grid upgrades, see Guidelines for Scheduling Full Upgrades.
Deleting Files From a Member

Viewing Files

- Viewing Files from the Files Tab
- Viewing Files from the Members Tab

Managing Users

- Users Default Home Directory
- Enabling FTP Anonymous User
- Adding FTP Users through Grid Manager
- Adding FTP Users through CSV Import
- Modifying FTP Users

File Distribution Overview

You can upload files to the NIOS appliance and to individual Grid members using TFTP, HTTP, and FTP clients. You can also upload files using the Grid Manager web interface or the API. Using access control lists, you can specify which network devices can upload files or retrieve files. You can use the Group Results function for file distribution services (TFTP, FTP, and HTTP) to group members by extensible attributes that contain the same values. For information about how to group members by extensible attributes, see Grouping Members by Extensible Attributes.

Note: File distribution services using TFTP, HTTP, and FTP is not supported by IPv6-only appliances.

Network devices, such as VoIP phones, can use the DHCP services on the appliance for IP address assignments and use the file distribution services for IP device configuration downloads. Downloads can be accomplished with TFTP, HTTP, or FTP.

Figure 9.1 Uploading and retrieving files

File uploads and downloads by FTP and TFTP file distribution clients are logged in the syslog under the Administration -> Logs tabs. The logs store the following information:

- Client IP
- Date and Time
- Event type
- File(s) downloaded and/or uploaded

File Distribution Storage

This section describes the storage capacity for file distribution, and how to manage file distribution storage settings. Maximum storage space allowed for all file distribution services on a Grid is equal to the storage space allowed on the Grid member with the smallest amount of space allowed. For example, if a Grid has a Riverbed member, which has a maximum limit of 1GB file distribution storage, then the maximum storage capacity you can set at the Grid level is 1GB, even if the Grid includes appliances with maximum limits of 10GB.

Maximum storage space is shown in table Table 9.1.

Table 9.1 Maximum Storage Space by Platform Type

<table>
<thead>
<tr>
<th>Member Type</th>
<th>Description</th>
<th>Max Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFOBLOX_MEMBER</td>
<td>All Infoblox appliances</td>
<td>10GB</td>
</tr>
<tr>
<td>VNIOS_MEMBER</td>
<td>All virtual appliances (VMWare)</td>
<td>5GB</td>
</tr>
<tr>
<td>VM_MEMBER</td>
<td>Virtual IPAM member (IPAM Free Ware)</td>
<td>1GB</td>
</tr>
</tbody>
</table>

Usage Threshold Alerts

An SNMP trap generates an alarm message when a member nears storage capacity. The default threshold value is 90%, and the default reset value is 70%. If email notification is enabled, NIOS sends an email when either of these thresholds are reached.

- When the Grid member storage capacity reaches 100%, the SNMP trap generates a “High Usage” message. For information on how to
Modify the threshold values, see Defining Thresholds for Traps.

- File distribution clients will fail to PUT files if the file is large enough that it will put the member over the storage limit.

Modifying File Distribution Storage Limits

1. From the Data Management tab, select the File Distribution tab, and then click Grid File Distribution Properties from the Toolbar.
2. In the Grid File Distribution Properties editor, complete the following:
   - Storage Limit (MB): Enter the maximum storage space in megabytes.
   - Include files and directories in system backup: This is selected by default to ensure that the appliance includes the uploaded files in the backup. You can clear this check box to improve the backup performance if you have stored these files separately.
3. Save the configuration and click Restart if it appears at the top of the screen.

Note: To avoid data loss, after you change the storage limit FD services will be disrupted briefly and will take some time to resume. Wait until the File Distribution services are running again on the members before you upload any files.

Managing File Distribution Services

This section describes how to configure file distribution services such as TFTP, FTP and HTTP. This section also describes how to configure access control lists which determine which clients are granted access to the service, and which clients are denied access to the service.

Configuring the TFTP Service

The TFTP file distribution service is disabled on the appliance by default. To allow file distribution access using TFTP, you must specify the clients that are allowed to use the service and then enable the service on the appliance. If you do not specify this information or enable the service, the appliance denies access to all clients. The appliance provides read-only access to the files.

To configure the TFTP file distribution service on a member:

1. From the Data Management tab, select the File Distribution tab -> Members tab -> member check box, and then click the Edit icon.
2. In the Member File Distribution Properties editor, select the TFTP tab, and then complete the following:
   - Listen on Port: Enter the number of the port on which the appliance receives TFTP file distribution requests. The default is port 69.
   - Allow file transfers from: Configure the appliance to grant or deny permissions to TFTP file distribution requests from clients, as described in Configuring Access Control for File Distribution.
3. Save the configuration and click Restart if it appears at the top of the screen.

After you configure the TFTP service, you must enable the service to allow file distribution access. For information, see Starting and Stopping File Distribution Services.

Configuring the FTP Service

The FTP file distribution service is disabled on the appliance by default. To allow file distribution access using FTP, you must create at least one user (see Managing Users), specify the clients that are allowed to use the service, and then enable the FTP service on the appliance. If you do not specify this information or enable the service, the appliance denies access to all clients. User creation is not necessary to access the FTP service if anonymous is enabled at Grid level. The appliance provides read-only access to the files.

To configure the FTP file distribution service on a member:

1. From the Data Management tab, select the File Distribution tab -> Members tab -> member check box, and then click the Edit icon.
2. In the Member File Distribution Properties editor, select the FTP tab, and then complete the following:
   - Listen on Port: Enter the number of the port on which the appliance receives FTP file distribution requests. The default is port 21.
   - Login Banner: Enter your own login banner text that appears after you establish an FTP connection or use the default (Restricted Access Only).
   - FTP Passive Mode: By default, this is selected to enable FTP in passive mode; otherwise, it is in active mode. An FTP connection between a client and server can be in active or passive mode. In active mode, the server initiates the data connection. In passive mode, the client initiates the data connection. Depending on your firewall policy, firewalls can block active mode connections. There is no firewall filtering in passive mode.
   - FTP File Listing: Select this to allow users to list files and subdirectories on the appliance.
   - Allow file transfers from: Configure the appliance to grant or deny permissions to FTP file distribution requests from clients, as described in Configuring Access Control for File Distribution.
3. Save the configuration and click Restart if it appears at the top of the screen.

Enabling FTP Anonymous User

The 'anonymous' FTP login is disabled by default, except when upgrading an earlier version in which case anonymous FTP is automatically enabled.

When you enable anonymous FTP at Grid level, you enable anonymous FTP on all Grid members running the FTP service. Anonymous user is only allowed to download files, even if the member is enabled to allow uploads.

1. From the Data Management tab, select Grid File Distribution Properties on the toolbar.
2. In the Grid File Distribution Properties dialog box, select the Enable Anonymous FTP check box.
3. Click Save & Close.
Configuring the HTTP Service

To allow file distribution access using HTTP, you must specify clients that can request the service and then enable the HTTP service on the appliance.

Before you enable the HTTP service, however, be aware of the following configuration rules:

- HTTP only runs on the active member of an HA pair.
- HTTP can run on the master or any member.
- HTTP always runs on the LAN port, never the MGMT port.
- HTTP to HTTPS redirect becomes non-functional if the file distribution service is enabled and all administrative access is run on the LAN port. For more information on HTTP redirect, see Enabling HTTP Redirect. For information on how to specify the MGMT port for HTTP, see Using the MGMT Port. To configure the HTTP file distribution service on a member:

1. From the Data Management tab, select the File Distribution tab -> Members tab -> member check box, and then click the Edit icon.
2. In the Member File Distribution Properties editor, select the HTTP tab, and then complete the following:
   - Allow Any: This is selected by default to allow HTTP file distribution requests from any client.
   - Only these addresses: Select this to configure the access control list for allowing HTTP file distribution requests from clients, as described in Configuring Access Control for File Distribution.
3. Save the configuration and click Restart if it appears at the top of the screen.

Configuring Access Control for File Distribution

You can select a named access control list (ACL) or create individual access control entries (ACEs) for each file distribution service (TFTP, FTP, HTTP) to control access to file distribution requests from specific clients. You can grant or deny access from specific IPv4 addresses and IPv4 networks, but you cannot do so for IPv6 addresses and IPv6 networks as well as TSIG key based ACEs.

Note: For HTTP service, you can grant permissions to all clients or specific clients, but you can deny permissions only to all clients, not specific clients.

When you grant access to a network for a specific file distribution service, all clients in the network are allowed to request file distribution service. You can deny services to specific IP addresses within the network by adding these addresses to an access control list and denying access to the service. Ensure that you list these IP addresses before the network address in the list because the appliance applies permissions to the addresses in the order they are listed. You can use the arrow keys to move the addresses up and down the list after you add them. For information about how to create a named ACL, see Configuring Access Control.

To configure an access control list for a file distribution service:

1. From the Data Management tab, select the File Distribution tab -> Members tab -> member check box, and then click the Edit icon.
2. In the Member File Distribution Properties editor, select a service tab: TFTP, FTP, or HTTP.
3. In the Allow these clients to perform file transfers section, select one of the following:
   - For TFTP and FTP: None: Select this to deny any clients from using the TFTP and FTP file distribution services. This is selected by default.
   - For HTTP: Any: Select this to allow any clients to use the HTTP file distribution service. This is selected by default.
   - Named ACL: Select this and click Select Named ACL to select a named ACL that contains only IPv4 addresses and networks. File distribution does not support IPv6 addresses/networks and TSIG key based ACEs. When you select this, the appliance allows clients that have the Allow permission in the named ACL to use the file distribution service. You can click Clear to remove the selected named ACL.
   - Set of ACEs: Select this to configure individual access control entries (ACEs). Click the Add icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding.
     - IPv4 Address: Select this to add an IPv4 address. Click the Value field and enter the IP address. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.
     - IPv4 Network: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
       - Address: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
       - Permission: Select Allow or Deny from the drop-down list.
     - Any Address/Network: For TFTP and FTP only. Select this to allow or deny access to all IPv4 addresses and networks. The default permission is Allow, which means that the appliance allows access to and from all IPv4 clients. You can change this to Deny to block access. After you have added access control entries, you can do the following:
       - Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL icon and enter a name in the Convert to Named ACL dialog box. The appliance creates a new named ACL and adds it to the Named ACL panel. Note that the ACEs you configure for this operation stay intact.
       - Reorder the list of ACEs using the up and down arrows next to the table.
       - Select an ACE and click the Edit icon to modify the entry.
       - Select an ACE and click the Delete icon to delete the entry. You can select multiple ACEs for deletion.
4. Save the configuration and click Restart if it appears at the top of the screen.
Modifying Access Control Lists

1. From the **Data Management** tab, select the **File Distribution** tab -> **Members** tab -> *member* check box, and then click the Edit icon.
2. In the **Member File Distribution Properties** editor, select the tab of the service to which the list belongs.
3. In the **Allow file transfers from** section, modify the fields as described in *Configuring Access Control for File Distribution*.

You can also do the following:

- Add a new permission. For information, see *Configuring Access Control for File Distribution*.
- Delete a permission by selecting it and clicking the Delete icon.
- Reorder the list by selecting a permission and clicking an arrow next to the list to move the permission up or down the list.

Starting and Stopping File Distribution Services

You can enable and disable a file distribution service on a specific Grid member or on multiple members. You must have read/write permission to the Grid members to start and stop a service on them.

**Starting a service on a member:**

1. From the **Data Management** tab, select the **File Distribution** tab -> **Members** tab -> *member* check box, and then click the Start icon from the Toolbar. You can select multiple members by selecting their check boxes.
2. From the Start drop-down menu, select the service you want to start.
3. In the **Start Service** dialog box, click **Yes**.
   Grid Manager enables the selected service on the selected member and displays the service status in the Status column in the panel.

**Stopping a service on a member:**

1. From the **Data Management** tab, select the **File Distribution** tab -> **Members** tab -> *member* check box, and then click the Stop icon from the Toolbar. You can select multiple members by selecting their check boxes.
2. From the Stop drop-down menu, select the service you want to stop.
3. In the **Stop Service** dialog box, click **Yes**.
   Grid Manager disables the selected service on the selected member and displays the service status in the Status column in the panel.

*Note:* When you start or stop a service, there may be a short delay before Grid Manager displays the correct status.

Monitoring File Distribution Services

To view the current status of the file distribution services:

1. From the **Data Management** tab, select the **File Distribution** tab -> **Members** tab.
2. Grid Manager displays the following information:
   - **Name:** The name of the Grid member.
   - **Address:** The IP address of the Grid member.
   - **Status:** The overall status of the file distribution services running on the member. You can mouse over on the field to view the status of each service. This field can display one of the following:
     - **Not Running:** All the file distribution services are disabled.
     - **Running:** One or more of the file distribution services are running properly.
     - **Warning:** The services are functioning properly. However, there are some issues, such as storage space has reached 90%, about the services.
     - **Error:** One or more of the services have service issues.
   - **Comment:** Information about the member.
   - **Site:** The location to which the member belongs. This is one of the pre-defined extensible attributes.

You can sort the information in ascending or descending order by columns. You can also print and export the information in this panel.

Managing Directories

You can create directories on the Grid Master and on Grid members, in which you can store your files. You can manage the directories in the following ways:

- Create a directory structure for file distribution, as described in *Adding Directories*.
- Modify the directory name and permissions, as described in *Modifying Directories*.
- Create a Virtual TFTP root directory, as described in *Creating a Virtual TFTP Root Directory*.
- View the directories, as described in *Viewing Directories From the Files Tab*.
Adding Directories

To add a directory:

1. From the **Data Management** tab, select the **File Distribution** tab -> **Files** tab.
2. Click the parent directory link, and then click **Add** -> **Directory** from the Toolbar.
3. Grid Manager adds a new directory to the parent directory and gives it the default name **NewDirectory**. You can modify the directory name and permissions, as described in **Modifying Directories**.

Modifying Directories

1. From the **Data Management** tab, select the **File Distribution** tab -> **Files** tab.
2. Select a directory check box and click the **Edit** icon.
3. The **Directory** editor provides the following tabs from which you can modify data:
   - **General**: You can modify the directory name here, except for the Root directory.
   - **Virtual TFTP Root**: You can add an IP Address, a Network or a Range of IP addresses to support VMware ESX hosts who need different PXE boot images based on where they are in the network.
   - **Permissions**: You can add or delete admin permissions in this tab. For information, see **About Administrative Permissions**.
4. Save the configuration and click **Restart** if it appears at the top of the screen.
   You can also select a directory and click the Delete icon to delete it.

**Note**: When you delete a directory, the appliance automatically removes all its contents in that directory.

Creating a Virtual TFTP Root Directory

This section describes how to create a Virtual TFTP root directory for a specific IP address, network, or range of IP addresses. Note that Virtual TFTP root is supported only for file downloads, but not for file uploads using TFTP client.

**Note**: Root directory can not be a virtual TFTP root.

1. From the **Data Management** tab, select the **File Distribution** tab -> **Files** tab.
2. Select the directory check box and click the **Edit** icon.
3. In the **Directory** editor select **Virtual TFTP Root**. Click the Add icon and select one of the following:
   - **IP Address**: This creates a virtual TFTP directory that the clients from a specified IP address will see as the root directory.
   - **Network**: This creates a virtual TFTP directory that the clients on a specified network will see as the root directory.
   - **Range**: This creates a virtual TFTP directory that the clients in a specified range of IP addresses will see as the root directory.
4. From the drop-down in the **Member** column, select the member on which to make the virtual TFTP root directory.
5. In the **Address/Network** column, enter a value:
   - **IP Address**: Enter the IP address of the client that will have access to the virtual TFTP root directory. This IP address must be on the allow list in the TFTP access control list.
   - **Network**: Enter a network address using the format 10.0.0.0/24. This allows all clients in that network to access the virtual TFTP root directory. This network address must be on the allow list in the TFTP access control list.
   - **Range**: Enter the first IP address in the range Address/Network column, and the last IP address in the range in the **End** column. This allows all clients in that range to access the virtual TFTP root directory. This range must be on the allow list in the TFTP access control list.
6. Click **Save & Close**. Click **Restart** if it appears at the top of the screen.
7. To create more virtual TFTP root directories, repeat Steps 3 through 5.

Viewing Directories From the Files Tab

1. From the **Data Management** tab, select the **File Distribution** tab -> **Files** tab.
2. Grid Manager displays the following information in the Root directory:
   - **Name**: The name of the directory or file.
   - **Type**: Depending on the file type, this can be **Directory** or **File**.
   - **Size**: The file size in B, KB, or MB depending on whether the file size crosses the unit limit or not. For example, if the file size is 1023, Grid Manager displays 1023 B. If the file size is 1025, Grid Manager displays 1 KB. For a directory, Grid Manager displays a dash (-).
   - **Date Modified**: The timestamp when the directory was last created or when the file was last modified.
3. Click the directory link to view files and directories in a specific directory. You can also do the following in this panel:
   - Sort the information in ascending or descending order by columns.
   - Use the breadcrumb to go to a specific directory.
   - Use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.
   - Create a quick filter to save frequently used filter criteria. For information, see **Using Quick Filters**.
Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see *Modifying Data in Tables*.

Print and export the information in this panel.

Add a directory or a file. For information, see *Adding Directories* and *Managing Files*.

Open and edit a directory. For information, see *Modifying Directories*.

### Managing Files

This section describes how to upload files using the Grid Manager or a file transfer client. You can upload files to the Grid Master or to individual members.

### Uploading Files

Some things to keep in mind when you upload files:

- When you use the Grid Manager to upload files, you can upload files only to the Grid Master, not to individual members of the Grid.
- To upload files to a member, you must use an FTP client, TFTP client or HTTP client. Files uploaded by file transfer clients to any member, will be synchronized back to Grid Master.
- The logs for file transfers using third party clients can be found in syslog.
- You can use a third party file transfer client to upload and retrieve files:
  - If the 'anonymous' login is enabled, you can retrieve files but this 'anonymous' user can not upload files even if the “Allow uploads” option is enabled.
  - If you create a user to use with a third party transfer client, this must be an FTP user with read/write permissions in their directory.
- You can upload a maximum of 10,000 files.
- If uploading the file exceeds the storage limit, the appliance logs a message and does not upload the file. For information about file distribution storage, see *Modifying File Distribution Storage Limits*.
- If you upload a file that has the same name and path as an existing file, the appliance automatically replaces the old file.

*Note:* Administrators with superuser privileges can manage uploading files. Limited-access admins with read/write permissions to specific directories can upload files to the directories. For information, see *Administrative Permissions for File Distribution Services*.

### Enabling Upload to Grid Members

1. From the **Data Management** tab, select Grid **File Distribution** Properties on the toolbar.
2. In the **Grid File Distribution Properties** dialog box, select the **Allow Upload to Grid Members** check box.
3. Click **Save & Close**.

### Uploading Files using Grid Manager

The Grid Manager uploads files only to the Grid Master. The Grid Master propagates the files to the members. You must use a third party file transfer client to upload files directly to an individual member:

- If the 'anonymous' login is enabled, you can retrieve files but this 'anonymous' user can not upload files even if the “Allow uploads” option is enabled.
- If you create a user to use with a third party transfer client, this must be an FTP user with read/write permissions in their directory.

1. From the **Data Management** tab, select the **File Distribution** tab -> **Files** tab.
2. Select the destination directory link.
3. Click the **Add** icon -> **File** from the Toolbar.
4. Select the **Extract files after upload (.zip, .tar, .gz, .tgz)** check box in the **Upload** dialog box if you are uploading .zip, .tar, .gz, or .tgz files and you want to automatically extract the files upon upload.

*Note:* The directory structure in the compressed file is restored when the files are extracted. A directory that already exists it will be replaced by an extracted directory with the same name.

5. Click **Select** to navigate to the file you want to upload.
6. Select the file you want to upload, and then click **Open**.
7. If you want to upload more than one file, repeat Steps 4 and 6 until you have selected all the files you want to upload. You can upload a maximum of ten files at one time.

*Note:* You can delete an incorrect file selection by clicking the red icon next to the filename before you click Upload.

8. To verify the upload was successful, roll the mouse cursor over the green check mark next to the file name. If the upload was successful, the message “Upload succeeded.” appears.
Uploading Files Using TFTP, FTP, or HTTP File Transfer Client

You can upload files to the Grid Master or to individual members using a third party FTP client. Files uploaded by file transfer clients to any member, will be synchronized back to Grid Master.

To upload files to a member, you must first enable the Allow Upload to Grid Members check box in the Grid File Distribution Properties dialog box. See Enabling Upload to Grid Members.

You must add an FTP user before you can upload files using a third party FTP client. This must be an FTP user. It is not the NIOS admin. For information see Adding FTP Users through Grid Manager.

Deleting Files From the Grid Master

If the FTP user has read/write permissions, then that user can delete files from the Grid member wherever that FTP user is connected. Only files can be deleted but not directories.

1. From the Data Management tab, select the File Distribution tab -> Files tab.
2. Grid Manager displays the files and folders in the Root directory. Click the directory link to see the files in a specific directory.
3. To delete a file, select the check box and then click the Delete icon.

Deleting Files From a Member

You can delete files from a member only if “No” appears in the Synchronized with Grid Master column.

If the FTP user has Read/Write permissions, then that user can delete files from the Grid member wherever that FTP user is connected. Only files can be deleted but not directories.

1. From the Data Management tab, select the File Distribution tab -> Files tab.
2. Grid Manager displays the files and folders in the Root directory. Click the directory link to see the files in a specific directory.
3. If “No” appears in the Synchronized with Grid Master column, select the check box, then click the Delete icon.

Viewing Files

You can view files from the Files Tab and from the Members Tab.

Viewing Files from the Files Tab

1. From the Data Management tab, select the File Distribution tab -> Files tab.
2. Grid Manager displays the following information in the Root directory.
   - Name: The name of the file.
   - Type: Depending on the file type, this can be Directory or File.
   - Size: The file size in B, KB, or MB depending on whether the file size crosses the unit limit or not. For example, if the file size is 1023, Grid Manager displays 1023 B. If the file size is 1025, Grid Manager displays 1 KB. For a directory, Grid Manager displays a dash (-).
   - Date Modified: The timestamp when the directory was last created or when the file was last modified.

You can view files and directories in a specific directory by clicking the directory link.

Viewing Files from the Members Tab

1. From the Data Management tab, select the File Distribution tab -> Members tab.
2. Grid Manager displays the following information in the Root directory.
   - Name: Member name.
   - IPv4Address: Member’s IP address.
   - Status: State of the member, running or not running.
   - Comment: Additional comments about the member.
   - Site: User defined information about the site.
3. To see the files on the Grid Master, click on the name of the Grid Master. Grid Manager displays the following information:
   - Name: The name of the file.
   - Type: Depending on the file type, this can be Directory or File.
   - Size: The file size in B, KB, or MB depending on whether the file size crosses the unit limit or not. For example, if the file size is 1023, Grid Manager displays 1023 B. If the file size is 1025, Grid Manager displays 1 KB. For a directory, Grid Manager displays a dash (-).
   - Date Modified: The timestamp when the directory was last created or when the file was last modified.

Tip: When you drill down on the Grid Master from the Members tab, the Add icon is activated.

4. To see the files on a member, click on the name of the member. Grid Manager displays the following information:
   - Name: The name of the file.
You can also do the following in this panel:

- Sort the information in ascending or descending order by columns.
- Use the breadcrumb to go to a specific directory.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
- Print and export the information in this panel.
- Add a directory or a file. For information, see Adding Directories and Managing Files.
- Open and edit a directory. For information, see Modifying Directories.
- You can enable “group by” function to organize your members in a meaningful way and quickly identify them based on common data.

Complete the following to group members with the same extensible attribute value:

- **Group Results:** Select this check box to enable the appliance to group members by extensible attributes.
- **Group By:** From the drop-down list, select the first extensible attribute that you want the appliance to use for filtering members.

Grid Manager displays data per group of members configured with the same extensible attribute value. For more information about grouping by extensible attributes, see Grouping Members by Extensible Attributes.

### Managing Users

This section describes how to add and modify user accounts for use with an FTP client.

You must be a NIOS admin user with super user privileges to add, modify, or delete FTP users. FTP users are created at Grid level, so the same users will be available to access FTP service on all members.

- Each user must have unique Username.
- By default, the home directory with the user name is under the /ftpusers directory. However, the user can also choose to use an existing directory outside of /ftpusers as his home directory. If the admin specified home directory is not available then it will raise an error.
- Permission: Read-write or Read-only are assigned for each FTP user. Users with read-write permissions are allowed to upload files, delete files and list the files and directories under his home directory.
- You can have multiple users to use same home directory. One user may have read-only permissions while others have read-write permissions on same home directory.
- FTP users are not allowed to add, modify, or delete the directories, even with read-write permissions.
- If the “Allow uploads on the member” is disabled, then users with read-write permission also can not upload files to his home directory.

### Users Default Home Directory

- FTP users default home directory is /ftpusers.
- The /ftpusers directory is created by default and listed in the ‘Files’ viewer under the root directory. By default, home directories for FTP users are under this directory.
- NIOS admin is allowed to upload and delete files to and from users home directories.
- Files uploaded by FTP users are visible in the Grid Manager.

### Adding FTP Users through Grid Manager

1. From the Data Management tab, select the File Distribution tab -> FTP Users tab, and then click the Add icon.
2. In the Add FTP User dialog box, complete the following:
   - **Username:** Enter a name for the user. This is the username that the user uses to log in.
   - **Password:** Enter a password for the user to use when logging in.
   - **Confirm Password:** Enter the same password.
   - **Permissions:** From the drop down choose from the following:
     - **Read Only:** This allows the user to display files, but not to upload, or delete files using a third party FTP client.
     - **Read/Write:** This allows the user to upload, delete and list files using a third party FTP client.
   - Choose a directory for this user. This is the directory where files uploaded with this Username will go:
     - **Create Home Directory:** This creates a directory using the Username.
     - **Choose Specified Directory:** This allows the user to choose an existing directory.
3. Click Save & Close.
Adding FTP Users through CSV Import

You can add an FTP User by importing a CSV file with the headers in the following format:

```
version 1.0,,
header-ftpuser,username*,password*,create_home_dir,home_dir,permission
ftpuser,user1,passwd1,True,/ftpusers/user1,RO
```

Modifying FTP Users

1. From the Data Management tab, select the File Distribution tab -> FTP Users tab.
2. Select the check box for the user you want to modify and click the Edit icon.
3. In the FTP User Editor you can modify the following:
   - **Password**: Enter a password for the user to use when logging in.
   - **Confirm Password**: Enter the same password.
   - **Permissions**: From the drop down choose from the following:
     - **Read Only**: This allows the user to display the files and their properties, but not to edit them.
     - **Read/Write**: This allows the user to display and edit the files and their properties.
4. Click Save & Close.

Chapter 10 Managing NIOS Software and Configuration Files

This chapter explains how to manage upgrade groups and perform software upgrades and downgrades for NIOS appliances. It also describes how to back up and restore configuration files. It includes the following sections:

- **About Upgrades**
  - Lite Upgrades
  - Full Upgrades
  - Guidelines for Scheduling Full Upgrades
  - Microsoft Management Rules
- **Managing Upgrade Groups**
  - Adding Upgrade Groups
  - Modifying Upgrade Groups
  - Viewing Upgrade Groups
  - Deleting Upgrade Groups
- **Viewing Software Versions**
- **Upgrading NIOS Software**
  - Uploading NIOS Software
  - Distributing Software Upgrade Files
  - Managing Distributions
  - Testing Software Upgrades
  - Performing Software Upgrades
  - Managing Upgrades
  - Monitoring Distribution and Upgrade Status
- **Downgrading Software**
- **Reverting the Grid to the Previously Running Software**
- **Applying Hotfixes**
- **Backing Up and Restoring Configuration Files**
  - Backing Up Files
  - Automatically Backing Up Data Files
  - Manually Backing Up Data Files
  - Downloading Backup Files
  - Restoring Backup Files
  - Downloading Backup Files from a Different Appliance
- **Using Database Snapshots**
  - Creating Database Snapshots
  - Rolling Back Database Snapshots
  - Downloading Support Bundles

**About Upgrades**

Infoblox frequently releases updated NIOS software. Contact Infoblox Technical Support to learn which file name to use when downloading a new upgrade file, or watch your email for periodic notifications that a new software upgrade is available. To get the latest upgrade, your local network must be capable of downloading a file from the Internet. For information about how to upgrade, see [Upgrading NIOS Software](#).

You can upgrade an appliance to a specific release if the current release on your appliance supports the upgrade path. For information about the upgrade and revert paths of a specific release, refer to the latest release notes at [https://support.infoblox.com](https://support.infoblox.com). Depending on whether there are database schema changes between the existing and upgrade releases, the appliance can perform either a lite or full upgrade. For information, see [Lite Upgrades](#) and [Full Upgrades](#).

You can schedule certain upgrades for a Grid. Scheduling an upgrade can minimize network and operational outages, especially when Grid members are spanned across different time zones. You can also arrange the upgrade to happen during non-peak hours for specific members to avoid overloading the network traffic. When you schedule an upgrade, you can schedule to update all Grid members at the same time or at
different times. Depending on the configuration of your Grid and the software version that is currently running in the Grid, you can also schedule your upgrades for different members over a period of time. For more information, see Scheduling Upgrades. Based on your network requirements and topology, you can organize your members into upgrade groups so these members can be upgraded at the same time. For more information about upgrade groups, see Managing Upgrade Groups. You can also import and export upgrade groups and their distribution and upgrade schedules in CSV format. For information about how to import and export in CSV format, see About CSV Import and Exporting Data to Files.

Note: When you promote a Grid Master candidate to a Grid Master, you cannot revert to the previous release. Also, your login username cannot contain any uppercase letters (A to Z), otherwise an upgrade will fail.

Lite Upgrades

A lite upgrade occurs when there are incremental changes to the software that do not require any upgrade to the database. The appliance can perform a lite upgrade only if the format of the database between the existing NIOS version and the upgrade version is the same. In general, when you upgrade from a patch release to another patch release, you are performing a lite upgrade. In a lite upgrade, members can be running a different software version than the Grid Master. You can add objects, such as zones, networks, and resource records to the members that are running an older NIOS version. Replication of zones, networks, resource records, and DHCP leases is supported between the Grid Master and members. When you want to revert a member however, you must revert the entire Grid. Whenever possible, the appliance uses the lite upgrade mode to speed up the upgrade process. You can always schedule a lite upgrade. Note that the appliance disables the testing function for lite upgrades because you do not need to test a lite upgrade for any database translation. For information about how to schedule an upgrade, see Scheduling Upgrades.

Full Upgrades

A full upgrade occurs when there are database schema changes between the existing and upgrade releases. In general, when you upgrade to a major release, you are performing a full upgrade. Depending on the upgrade and revert paths that your existing release supports, you may or may not be able to schedule a full upgrade. A full upgrade that cannot be scheduled does not allow for data replication between the Grid Master and members. For information about supported upgrade and revert paths, refer to the latest release notes on the Infoblox Support site. Depending on the upgrade paths your current release supports, when you schedule a full upgrade, the Grid Master immediately replicates certain core network service tasks to Grid members while putting other tasks in queue until the members have been upgraded. For information about which data and tasks the Grid Master replicates to members immediately, see Guidelines for Scheduling Full Upgrades. For information about how to schedule an upgrade, see Scheduling Upgrades.

Guidelines for Scheduling Full Upgrades

When you schedule a full upgrade from NIOS 6.6.x or later to a later NIOS release, the Grid Master immediately replicates the following to the Grid members, including those that have not been upgraded:

- DNS resource records, DNS zones, DNS views, name server groups, shared record groups, IPv4 and IPv6 host addresses, roaming hosts, IPv4 and IPv6 networks, IPv4 and IPv6 shared networks, fixed addresses, DHCP ranges, DHCP failover association, DHCP option spaces, DHCP options, DHCP filters, MAG filter items, blacklist & NXDOMAIN rules, DNSSEC key pairs, DNSSEC import keyset operation, sign and unsign zones, DNSSEC rollover KSK and ZSK operations.

You can also perform the following tasks:

- Upgrade a specific member during the scheduled Grid upgrade. For information about how to upgrade a single member during a scheduled Grid upgrade, see Upgrading a Single Member Immediately.
- Revert a single member that has already been upgraded so you can troubleshoot issues, such as service outages, on the specific member. You can then reschedule its upgrade. For more information, see Reverting a Single Member.
- Clear authentication cache and authentication records.
- Perform AD (Active Directory) configurations. Note that you must upload the keytab file before the upgrade starts.

When you schedule a full upgrade for your Grid, ensure that you understand the following restrictions related to service restarts:

- When upgrading from NIOS 7.1.x or earlier releases to any NIOS releases, you will not be able to restart services on Grid members that have not been upgraded.
- When you upgrade from NIOS 7.2.7 or earlier 7.2.x releases to NIOS 7.3.3 and earlier 7.3.x releases, you will not be able to restart services on Grid members that have not been upgraded. If necessary, you may use the restart service CLI command to manually restart services on the Grid members that have not been upgraded.
- When you upgrade from NIOS 7.2.7 and earlier 7.2.x releases to NIOS 7.2.8 and later releases or NIOS 7.3.4 and later releases, you will be able to restart services.

Note: Note that the service restart restriction does not exist for future scheduled full upgrades once your Grid has been upgraded to NIOS 7.3.0 and later 7.3.x releases.

The appliance also puts certain rules in place to ensure data integrity and controls data that can cause undesirable results during the upgrade process. When you schedule a full upgrade from NIOS 6.6.x or later to a later NIOS release, the following rules apply:

- You cannot modify member properties for the following: DNS, DHCP, TFTP/HTTP/FTP, bloxTools, Captive Portal, Reporting, and load balancing until the member has completed the upgrade and exited its revert time windows.
- You cannot delete DNS views.
- You cannot delete DNS zones and IPv4 and IPv6 networks that are under Microsoft Management until the managing member of the Microsoft servers has completed its upgrade and exited its revert time window. Certain Microsoft management restrictions also apply, as described in Managing Upgrade Groups.

Copyright ©2019, Infoblox, Inc. All right reserved.
- Synchronization between load balancers and the appliance is disabled until the load balancer managing member has completed its upgrade and exited its revert time window. You cannot change the managing member during the upgrade.
- You cannot add, modify, or delete network views, rulesets, and DNS64 synthesis groups.
- Replication of Grid and member DNS and DHCP properties is not supported.
- You can create named ACLs (access control lists) only after the entire Grid has been upgraded. For information about named ACLs, see Configuring Access Control.

Note that during a scheduled full upgrade, you cannot perform the following tasks on a Grid member that has not been upgraded yet:

- Start or stop the DNS and DHCP services on members that have not been upgraded, have been reverted, or are in the revert time window.
- Import the DHCP lease history file
- Use the DHCP expert mode configuration feature
- Clear the NAC authentication cache of a DHCP member
- Set the time zone for a Grid member
- View the capacity report of a Grid member
- Test the email configuration settings of a Grid member
- Check whether an IPv6 address is already configured on a Grid member

When you schedule a full upgrade from a previous NIOS release to a release that includes the DHCP fingerprint detection feature, the following rules apply until the entire Grid has been upgraded:

- DHCP fingerprint detection is disabled
- You cannot add DHCP fingerprint filters
- You cannot apply DHCP fingerprint filters to any DHCP address range

When you schedule a full upgrade from a previous NIOS release to a release that includes the multi-primary zone feature, the following rules apply until the entire Grid has been upgraded:

- You cannot configure multiple primary servers for an authoritative zone or configure a name server group that contains multiple primary servers.
- You cannot assign or unassign a Grid member to an authoritative zone or name server group.
- You cannot change the stealth state of an authoritative zone or name server group.

When you schedule a full upgrade from a previous NIOS release to a release that includes the Infoblox Threat Protection feature, you cannot complete the following on a Grid member until the member has completed the upgrade:

- Start or stop the Threat Protection and DNS services.
- Activate a ruleset.
- Perform any threat protection related tasks such as adding custom rules and activating rulesets.

Before scheduling a full upgrade from a previous NIOS release to a release that includes the IPv6 Grid feature, the following rules apply:

- If the Grid has an HA Master or HA member and if it is configured with IPv6 VIP address, you must configure IPv6 addresses for both node 1 and node 2.
- Both the Grid Master and the Grid Master Candidate should have the same type of network connectivity.
- You have to back up the current configuration and database.

When you schedule a full upgrade from a previous NIOS release to a release that includes the Secure Dynamic Updates feature, the following rules apply until the Grid has completed the upgrade:

- All dynamic updated records are labelled as static records. Infoblox suggests that you enable this feature only after all records are changed to Dynamic.
- NIOS tags the RRsets that are not auto-generated as static records. For information about Secure Dynamic Updates, see Secure Dynamic Updates.

When you schedule a full upgrade from a previous release to NIOS 7.2.x or 7.3.x, the following rules apply until the entire Grid has been upgraded:

- You cannot add, modify, or delete an NS group.
- You cannot add, modify, or delete manually created NS records.
- You cannot add, modify, or delete a zone.
- You cannot assign or unassign an NS group to a zone.
- You cannot change the NS group assigned to a zone.
- You cannot change the host name of the Grid members that are assigned to a zone if the members have not been upgraded, have been reverted, or are in the revert time window.
- You cannot restart DNS and DHCP services or schedule a restart for these services on Grid members that have not been upgraded. For more information, see Restarting Groups.

Note the following when you schedule a full upgrade from a previous release to NIOS 7.2.x and later:

- You cannot start or stop the DNS and DHCP services.
- You must not modify the settings for automated mitigation of phantom domain attacks using the CLI commands on a Grid member until the member has completed the upgrade. Otherwise, the changes made during the upgrade may get lost.

When you schedule a full upgrade from a previous NIOS release to NIOS 7.3.x or later that includes the DNS Traffic Control feature, the following
rules apply until the entire Grid has been upgraded:

- You cannot add an SNMP health monitor.
- You cannot configure the All available load balancing method for a DTC pool.
- The record types are reset to default record types (A and AAAA records) and you cannot modify the record types for an LBDN.

Note the following when you upgrade a Grid which includes members that support Infoblox Advanced DNS Protection:

- When you schedule a full upgrade from a previous NIOS release to NIOS 7.3.x or later, the Threat Protection Statistics widget in the Dashboard is replaced by the Threat Protection Status for Member widget. For information about the Threat Protection Status for Member widget, see Threat Protection Status for Member.
- When you schedule a full upgrade from NIOS 7.3.x release to NIOS 8.0.x and later releases, the Dig Request, Threat Analytics Status for Grid, and Threat Analytics Status for Member widgets will not be available in the Dashboard, by default. You have to add the widget to the Dashboard. But if you upgrade from NIOS 7.2.x or earlier releases to NIOS 8.0.x and later releases, the Dig Request, Threat Analytics Status for Grid, and Threat Analytics Status for Member widgets will be available in the Dashboard, by default. For information about the Dig Request, Threat Analytics Status for Grid, and Threat Analytics Status for Member widgets, see Dig Request, Threat Analytics Status for Grid, and Threat Analytics Status for Member respectively.

Microsoft Management Rules

On a member that synchronizes data with Microsoft DNS and DHCP servers, the following functions are deactivated during an upgrade:

- Synchronization of Microsoft DNS and DHCP data
- Rotation of Microsoft logs
- Start and stop of Microsoft servers
- Releases of DHCP leases from a Microsoft DHCP server

Note: Note that the deactivation of these functions does not affect any data on the Microsoft servers. After the upgrade, the member automatically restarts the synchronization of Microsoft data.

On a member that synchronizes data with Microsoft DNS and DHCP servers, the following rules apply:

- You cannot modify the managing member if the old and new members have not been upgraded and have not exited their revert time windows.
- You cannot add, modify, or delete zones, IPv4 DHCP ranges, and IPv4 networks until the managing member has been upgraded and exits the revert time window.
- You cannot add, modify, or delete DNS resource records if the associated zone is managed by a Microsoft server and the managing member is still in its revert time window.
- You cannot add, modify, or delete fixed addresses that are assigned to a Microsoft server and the managing member is still in its revert time window.
- You must wait until the new managing member is upgraded to configure it as a DNS primary or secondary.

Managing Upgrade Groups

To minimize the impact of Grid upgrades on your system operations, you can organize members into upgrade groups and schedule their software distributions. This is useful, for example, in a large Grid spanning multiple time zones where there are fluctuating network and downtime considerations at various locations. Note that you can also schedule their upgrades, depending on the existing releases and their upgrade paths. For information about the different upgrade methods, see About Upgrades.

You can also import and export upgrade groups and their schedules in CSV format. For more information, refer to the Infoblox CSV Import Reference.

Infoblox provides two default upgrade groups:

- Grid Master: After you configure the Grid Master, it automatically becomes the only member of this group. You cannot modify or delete this group.
- Reporting Member: After you configure a reporting member in a Grid, it automatically becomes the only member of this group. This group will be upgraded automatically after the Grid Master and before other upgrade groups. You cannot modify, delete, or schedule this upgrade group. For information about reporting, see Infoblox Reporting and Analytics.
- Reporting Member (when you have configured reporting clustering Grid): When you upgrade from NIOS 7.3.200 to a later release, the Grid will be upgraded to the single indexer mode. You can change the configuration after the upgrade. During an upgrade, the reporting members of the primary site are moved into separate groups to ensure that there are always some peers available to receive events sent by the forwarders. To achieve this, the replication factor must be equal to the search factor and the total number of reporting appliances.

Note: During an upgrade, data loss might happen if the peers that hold all searchable copies of a bucket are in the same group and they are all offline at the same time. To avoid this, ensure that you group the members in separate groups.

- Default: This is the default upgrade group to which the appliance automatically assigns Grid members. If you do not explicitly assign a member to an upgrade group, it remains in the Default group. You cannot delete or rename this group. For information, see Modifying Upgrade Groups.

Note: Make sure that the default group has at least one member associated with it, otherwise the appliance displays that the upgrade process is still in progress even though it is complete. To avoid this, you can either use the Infoblox > set grid_upgrade
Grid Manager provides information about the upgrade group to which a member belongs. You can add or delete an upgrade group and monitor the software version that is currently running on the Grid and on individual member. You can do the following:

- Add an upgrade group, as described in Adding Upgrade Groups.
- Modify an upgrade group, as described in Modifying Upgrade Groups.
- View upgrade group information, as described in Viewing Upgrade Groups.
- Delete an upgrade group, as described in Deleting Upgrade Groups.

Adding Upgrade Groups

When you create an upgrade group, you select the Grid members for that group, and specify whether the software distribution and upgrade occur on all group members at the same time, or successively in the order they are listed in the group members list. A Grid member can belong to only one upgrade group.

**Note:** The appliance displays a warning message when you create an upgrade group that includes the two peers of a DHCP failover association. Infoblox recommends that you assign DHCP failover peers to separate upgrade groups to minimize the risk of a loss in DHCP services. For example, if DHCP failover peers are in the same upgrade group and its members upgrade simultaneously, the upgrade causes a loss in DHCP services.

Note the following recommendations when you create an upgrade group:

- Put the following members in the first upgrade group after the Grid Master upgrade: all Grid Master candidates, DNS primaries, and the DHCP logging member.
- To minimize the risk of a loss in DNS services, put the name servers for a zone in different upgrade groups, and assign the primary and secondary servers to separate upgrade groups.

To add an upgrade group:

1. From the Grid tab, select the Upgrade tab.
2. Click Toggle Group List View to display the list of upgrade groups, and then click the Add icon.
3. In the Add Upgrade Group wizard, complete the following:
   - **Name:** Enter a name for the upgrade group. The name can contain alphanumeric characters, spaces, underscores, hyphens, and dashes.
   - **Distribute to Members:** Select one of the following to specify how the Grid Master distributes software to the members in the group.
     - **Simultaneously:** Select this to distribute software upgrade files to all group members at the same time.
     - **Sequentially:** Select this to distribute software upgrade files to group members in the order they are listed in the group members list.
   - **Upgrade Members:** Select one of the following to specify how the group members upgrade to the new software version.
     - **Simultaneously:** Select this to upgrade all group members at the same time.
     - **Sequentially:** Select this to upgrade group members in the order they are listed in the group members list.
   - **Comment:** Enter useful information about the upgrade group, such as the location of the group.
4. Click Next to select members for the group. Complete the following:
   - Click the Add icon. Grid Manager adds a row to the Member Assignment table.
   - Click Select. In the Member Selector dialog box, select the members you want to add to the group, and then click the Select icon. Use Shift+click and Ctrl+click to select multiple members. Note that if you choose to distribute and upgrade members sequentially, the distribution and upgrade occur in the order the members are listed. You can reorder the list by dragging a member to a desired location or by selecting a member and using the up and down arrows next to the check box to place the member at a desired location. You can also delete a member from the list.
   - **Note:** After you add a member, the appliance adds it to the group members list. The first Grid member in the list determines the time zone of the group when you schedule the distribution and upgrade. Therefore, Grid Manager displays the time zone of the first Grid member in the list. (For information about setting time zones, see Managing Time Settings.)
5. Save the configuration and click Restart if it appears at the top of the screen.

Modifying Upgrade Groups

You can modify an existing upgrade group to change the group name or how the distribution and upgrade are performed. You can also add and delete members.

To modify an upgrade group:

1. From the Grid tab, select the Upgrade tab, and then click Toggle Group List View.
2. Select an upgrade_group check box, and then click the Edit icon in the row. You can also click the Edit icon directly without selecting the check box.
3. The Upgrade Group editor provides the following tabs from which you can modify data:
   - **General:** Modify the fields as described in Adding Upgrade Groups.
   - **Member Assignment:** Add or delete members as described in Adding Upgrade Groups.
4. Save the configuration and click Restart if it appears at the top of the screen.

Viewing Upgrade Groups

In the Upgrade tab, Grid Manager lists the Grid Master group, the Default group, and other upgrade groups you have configured. You cannot modify or delete the Grid Master group. You can modify the Default group, but you cannot delete it. To view the members in a specific upgrade group, click the arrow next to the group name to expand the group. All groups are collapsed by default. Before a distribution or upgrade starts, you can move members from one group to another, reorder the members, or remove a member from an upgrade group. The member you remove automatically joins the Default group. (For information, see Managing Distributions.) You cannot add, delete, or reorder members in an upgrade group while a distribution or upgrade is in progress. You can skip a member in an upgrade group from a distribution only before the distribution starts, or after you pause it. For information, see Pausing and Resuming Distributions.

To view the upgrade groups in a Grid:

1. From the Grid tab, select the Upgrade tab, and then click Toggle Group List View. Grid Manager displays the Grid Master at the top of the list. All other upgrade groups are listed alphabetically after the Grid Master. You can click the arrow next to a group to view members in the group.
2. Grid Manager displays the following:
   • Group: The name of an upgrade group to which the member belongs.
   • Member: The name of the member.
   • Status: Displays the overall status of an upgrade group at the group level and individual status for each member when you expand the upgrade group. At the group level, this displays the most severe status among the members. For example, when there are three out of five members are offline, the overall status shows 3 of 5 members in red, which means offline.
   • IP Address: The IP address of the member.
   • Running Version: The NIOS software version that is currently running on the member.
   • Distribution Status: The distribution status of the group.
   • Timestamp: The date, time, and time zone when a distribution or upgrade is complete.

You can hide some of the default columns, but you cannot sort the information in this table. You can use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches. You can also create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.

Deleting Upgrade Groups

When you delete an upgrade group, members in the upgrade group that you want to delete will be moved to the Default group. Grid Manager displays a warning before deleting an upgrade group.

To delete an upgrade group:

1. From the Grid tab, select the Upgrade tab, and then click Toggle Group List View.
2. Select an upgrade-group check box, and then click the Delete icon.
3. In the Delete Confirmation dialog box, click Yes.

Viewing Software Versions

Before you upgrade, downgrade, or revert to a different NIOS software version, you can view the current software version that is running on the Grid, the NIOS image you have uploaded, and the available version to which you can revert. Grid Manager displays the software information in the Upgrade tab.

To view software information:

1. From the Grid tab, select the Upgrade tab.
2. Grid Manager displays the following in the Grid Version Information section:
   • Running: The NIOS software version that is currently running on the Grid.
   • Uploaded: The latest NIOS image file you have uploaded and is available for distribution.
   • Distribution: The NIOS software version used for distribution or is available for distribution.
   • Revert: The NIOS software version to which the appliance can revert.
   • Distribution Schedule: Displays the date and time of the next scheduled distribution.
   • Upgrade Schedule: Displays the date and time of the next scheduled upgrade.

Note: Grid Manager leaves a field empty when there is no available software for the specific function.

Grid Manager automatically refreshes the Upgrade tab with the latest information and displays the timestamp in the Last Updated field below the Grid Version Information section.

Upgrading NIOS Software

Infoblox frequently releases updated NIOS software. Contact Infoblox Technical Support to learn which file name to use when downloading a new upgrade file, or watch your email for periodic notifications that a new software upgrade is available. To get the latest upgrade, your local network must be capable of downloading a file from the Internet.

After you download and store the new upgrade file on your local network, complete the following tasks to upgrade an Infoblox independent appliance or a Grid.
Before upgrading, Infoblox recommends that all members in the Grid be connected to the network and operating normally. If one or more members are offline when you upgrade the Grid, they automatically receive the distributed software and upgrade when they join the Grid or come back online.

Note: You cannot upgrade directly to NIOS 5.x from NIOS releases less than 4.2r4. Refer to the release notes for the appropriate upgrade and revert paths.

Before you upgrade to a later NIOS release, use the show upgrade_compatible command to check if your Grid is compatible with the release. For information about using this command, refer to the Infoblox CLI Guide.

Caution: Do not attempt to add or remove a member, or convert an HA pair to single members or vice versa during a distribution or upgrade.

When you upgrade from NIOS 6.4.0 to a later release, you can start, stop, or restart DNS and DHCP services, or only the DHCP service on a member that has not been upgraded. When you start, stop, or restart other services, such as reporting or file distribution, the operation is put in queue for execution until after the targeted member has been upgraded.

**Uploading NIOS Software**

After you download the NIOS software upgrade to your management station, upload it to the Grid Master, as follows:

1. From the Grid tab, select the Upgrade tab, and then click Upload in the panel or from the Toolbar.
2. Navigate to the directory where you have stored the NIOS software upgrade, and then click Open or Upload.

The appliance uploads the file and displays the status of the upload in the status bar. You can click the Stop icon in the status bar to stop the upload. Ensure that you do not navigate away from the Upgrade tab until after the upload is complete. Otherwise, the upload process stops.

Note: When you upload the NIOS software upgrade to an HA Grid Master, only the active node receives the software. The passive node does not. Therefore, if the Grid Master fails over before a distribution starts, you must upload the software again. If you do not, the distribution fails because the new active node does not have the uploaded software.

**Distributing Software Upgrade Files**

Distributing the software upgrade files involves unpacking the software files and loading the new software. When you perform a distribution, the NIOS appliance loads the new software code into an alternate disk partition, which overwrites any previously saved version of code that is already there. Therefore starting the distribution disables the appliance from reverting to a release prior to the current version.

The time this process takes depends on the number of appliances to which the software is distributed; the more appliances, the longer it takes. Therefore, you might want to schedule the Grid distribution during times when your network is less busy. You can distribute the software immediately or schedule the distribution of any software upgrade file, even if it is not Upgrade Lite compatible.

**Distributing Software Immediately**

The Grid Master distributes the software upgrade to each member in the Grid, including itself. As an alternative to scheduling the Grid distribution (see Scheduling Distributions), you can distribute the software upgrade throughout the Grid immediately, as follows:

1. From the Grid tab, select the Upgrade tab, and then click Distribute -> Distribute Now from the Toolbar.
2. In the confirmation dialog box, click Yes to start the distribution.

The distribution starts and if there is an active distribution scheduled, the appliance changes its status to inactive. The appliance distributes the upgrade files and displays the status of the distribution in the status bar. You can pause, resume, or stop the distribution by clicking the corresponding icon in the status bar. For information, see Managing Distributions.

Note that starting a manual distribution cancels a scheduled distribution.

**Scheduling Distributions**

When you schedule a distribution, you schedule the distribution of the Grid Master as well as the upgrade groups, including the Default group. The Grid Master distribution must always occur before the distribution of the upgrade groups.

To schedule a software distribution:

1. From the Grid tab, select the Upgrade tab, and then click Distribute -> Schedule Distribution from the Toolbar.
2. In the Schedule Distribution editor, complete the following:
**Activate Distribution Schedule:** Select this to enable the distribution schedule. Clear this if you are creating a distribution schedule you plan to activate at a later date. You can configure and save information in this editor even when you deactivate a scheduled distribution.

**Grid Master Distribution Start Information:** Enter a Grid Master distribution date, time, and time zone. The distribution date and time must be before those of the upgrade groups.
- **Date:** Enter a start date of the Grid Master distribution in YYYY-MM-DD (year-month-day) format. You can click the calendar icon to select a date from the calendar widget.
- **Time:** Enter a start time of the Grid Master distribution in hh:mm:ss AM/PM (hour:minute:second in AM or PM) format. You can also select a time from the drop-down list.
- **Time Zone:** Select a time zone that applies to the start time you enter. If this time zone is different from the Grid time zone, the appliance converts the time you enter here based on the Grid time zone, after you save this schedule. When you display this schedule again, it displays the converted time. Selecting the time zone here does not affect any time zone settings in the Grid. (For information about selecting the Grid and member time zones, see Managing Time Settings.)
- **Admin Local Time:** Displays the Grid Master distribution start date and time in the time zone of the administrator, as explained in Creating Local Admins.

In the upgrade group table, specify the following for each upgrade group by clicking the corresponding field in each row:
- **Start Distribution:** Specify when the distribution occurs. Select one of the following from the drop-down list:
  - **Date/Time:** Select this to configure the distribution start date, time, and time zone.
  - **After <group>** : Select After Grid Master to start the distribution immediately after the completion of the Grid Master distribution. Select an upgrade group that must complete its distribution before the group you are configuring. When you select this option, you cannot enter a date, time, and time zone.
  - **Date, Time, and Time Zone** are enabled only when you select **Date/Time for Start Distribution**.
  - **Date:** Enter a distribution start date in YYYY-MM-DD (year-month-day) format. You can click the calendar icon to select a date from the calendar widget.
  - **Time:** Enter a distribution start time in hh:mm:ss AM/PM (hour:minute:second in AM or PM) format. You can select a time from the drop-down list.
  - **Time Zone:** By default, the appliance displays the time zone of the first Grid member in the Upgrade Group. You can change this time zone if you want to enter the time using a different time zone. After you save the schedule though, the appliance converts the time you entered to the time zone of the upgrade group, if it is different. (For information about setting the Grid and member time zones, see Managing Time Settings.) To change the default time zone of the upgrade group, change the time zone of the first group member, as explained in Adding Upgrade Groups.

- **Admin Local Time:** Displays the start date and time in the time zone of the administrator, as explained in Creating Local Admins.

- **Distribute to Members:** Indicates whether the distribution within the group occurs simultaneously or sequentially. You cannot edit this field here. You define this when you create the upgrade group. To change this setting, see Modifying Upgrade Groups.

3. **Save the configuration and click Restart** if it appears at the top of the screen.

Grid Manager confirms that the schedule is saved and indicates whether the distribution schedule is active. You can click the Refresh icon to refresh the information in this panel.

Note that the appliance does not save the schedule and displays an error message if the schedule contains the following:

- Circular dependencies between upgrade groups. For example, the distribution of Group A is scheduled after Group B, and the distribution of Group B is scheduled after Group A.
- The distribution time is in the past.

**Software Distribution Process**

The following series of events occur after a Grid distribution starts:

- The appliance checks if a NIOS software upgrade was uploaded.
  - If the upgrade files are not uploaded, the distribution stops. The appliance displays an error message and if the distribution is scheduled, the appliance deactivates the distribution schedule.
  - If the upgrade files are uploaded, the distribution proceeds.
- A single Grid Master uploads the file to a backup partition and unpacks the contents, which overwrites any existing backup software that might have been there. For an HA Grid Master, it is the active node that uploads the file to a backup partition and unpacks the contents. The Grid Master (or active node of the HA Grid Master) sends a command to all nodes that are online to copy their database and software to a backup software partition.
- For an HA Grid Master, the active node sends the command to the passive node as well.
- The nodes perform resynchronization on their backup partition, retrieving only the changed files from the Grid Master.
- After the active node of an HA member receives the software, it then distributes it to the passive node.

When the distribution successfully completes, the appliance updates the distribution status and sets the schedule, if configured, to inactive. The new software is now staged on all member appliances and is ready for use. Grid Manager displays the software version in the Distribution field in the Grid Version Information section.

**Managing Distributions**
After you start a distribution, you can pause, resume, or stop it. For information, see **Pausing and Resuming Distributions** and **Stopping Distributions**. Grid Manager displays the status of the overall distribution as well as the status of individual members. You can view this information in the **Upgrade** tab.

### Pausing and Resuming Distributions

The following are some operational guidelines for performing a distribution:

- You cannot create new upgrade groups, add members to a group, or remove members from a group after a distribution starts.
- You can skip a member that is currently offline from a distribution. When both nodes of an HA pair are online, the skip member function is not available.

To pause a distribution:

1. From the Grid Distribution Status bar, click the Pause icon.
2. When the appliance displays a confirmation dialog box, click **Yes** to pause the distribution.

The Grid Distribution Status bar indicates the distribution is paused. For information about the distribution status of each member, see **Monitoring Distribution and Upgrade Status**.

To skip a member from a distribution:

1. From the **Grid** tab, click the **Upgrade** tab, and then click **Toggle Member List View**.
2. Select a member check box, and then click **Skip Member** from the Toolbar. Grid Manager automatically skips the distribution of software to the members that are offline.

To resume a distribution:

1. From the Grid Distribution Status bar, click the Resume icon.
2. When the appliance displays a dialog box confirming that you want to resume the distribution, click **Yes** to continue.

Members that have not completed or started distributions that were scheduled at an earlier time resume the distribution.

### Stopping Distributions

You can stop a distribution immediately, for example, if there are offline members and you do not want to wait for them to come back online, or if you realize that you have uploaded the wrong software version. When you stop a distribution, you can do the following:

- If the Grid Master has completed its distribution, you can upgrade the Grid immediately. This forces members that do not have a complete distribution to synchronize their releases with the Grid Master.
- If the Grid Master does not have a valid distribution, you can restart the distribution.
- Upload another software upgrade.

Ending a distribution does not affect the upgrade schedule, if configured. The Grid upgrade starts as scheduled, as long as the Grid Master completes its distribution.

To stop a distribution:

1. From the Grid Distribution Status bar, click the Stop icon.
2. When the appliance displays a dialog box confirming that you want to stop the distribution, click **Yes** to continue.

### Testing Software Upgrades

After you successfully distribute a software upgrade to the Grid Master, you can test an upgrade on the Grid Master before actually implementing it. This allows you to resolve potential data migration issues before the actual upgrade. The length of time the upgrade test takes depends on the amount of data and the difference between the current NIOS version and the software upgrade. The test does not affect NIOS services and you can perform other administrative tasks during the upgrade test.

To start an upgrade test:

- From the **Grid** tab, select the **Upgrade** tab, and then click **Test Upgrade** from the Toolbar. Test upgrade is enabled only for a major upgrade (not an Upgrade Lite compatible upgrade).

After you start an upgrade test, you can view its status in the status bar. You can also stop it at anytime. To stop an upgrade test:

- From the **Grid Upgrade Test Status** bar, click the Stop icon.

Note that if an admin restarts the Grid services or reboots the Grid Master, or if an HA failover occurs on the Grid Master during the upgrade test, the appliance automatically stops the test. The appliance always resets the status of the Grid to “Distributed” when it stops the upgrade test.

If the appliance encounters an error during the test, it stops the test and displays a message in the **Upgrade Status** panel indicating that the upgrade test failed and the reason for the failure, such as a data translation error or data import error. You can review the syslog for specific error messages before downloading the Support Bundle and contacting Infoblox Technical Support.
After the test successfully finishes, the appliance displays a message confirming that the test upgrade is complete. You can then perform the actual upgrade as described in Performing Software Upgrades.

Performing Software Upgrades

Performing a software upgrade involves rebooting the appliances and then running the new software. Essentially, each appliance switches between the two software partitions on its system, activating the staged software and saving the previously active software and database as backup.

Note: Before you upgrade the software, Infoblox recommends that you back up the current configuration and database. For information, see Backing Up Files.

Depending on your upgrade paths, you can upgrade to a new release immediately or you can schedule the upgrade. For information about how to upgrade immediately, see Upgrading the Grid Immediately. Before you schedule an upgrade, ensure that you understand the limitations, as described in Managing Upgrade Groups. For information about how to schedule an upgrade, see Scheduling Upgrades.

Upgrading the Grid Immediately

For unschedulable full upgrades, all the Grid members in the Grid must upgrade at the same time. For lite upgrades and schedulable full upgrades, you can schedule the upgrades as described in Scheduling Upgrades, or you can upgrade all the Grid members at the same time. To upgrade a Grid immediately:

- From the Grid tab, select the Upgrade tab, and then click Upgrade -> Upgrade Now from the Toolbar.

Note: The Grid upgrades immediately and if there is an active upgrade schedule, it becomes inactive.

Scheduling Upgrades

You can schedule lite upgrades and full upgrades for certain NIOS versions. For limitations about scheduling a full upgrade, see Managing Upgrades of Groups. When you schedule an upgrade, you schedule the upgrade for the Grid Master and the upgrade groups, including the Default group. The Grid Master must always upgrade before the upgrade groups. Depending on your upgrade paths, you can schedule the upgrade for the Grid Master and upgrade groups at different times over a period of nine days. If you schedule an upgrade that takes more than nine days, the appliance displays a warning.

To schedule an upgrade:

1. From the Grid tab, select the Upgrade tab, and then click Upgrade -> Schedule Upgrade from the Toolbar.
2. In the Upgrade Schedule editor, complete the following:
   - **Activate Upgrade Schedule**: Select this to enable the upgrade schedule. Clear it if you are creating an upgrade schedule that you plan to activate at a later date. You can configure and save information in this editor even when you deactivate a distribution.
   - **Grid Master Upgrade Start Information**: Enter a Grid Master upgrade date, time, and time zone. The date and time must be before those of the upgrade groups.
     - **Date**: Enter a start date of the Grid Master upgrade in YYYY-MM-DD (year-month-day) format. You can click the calendar icon to select a date from the calendar widget.
     - **Time**: Enter a start time of the Grid Master upgrade in hh:mm:ss AM/PM (hour:minute:second in AM or PM) format. You can select a time from the drop-down list.
   - **Time Zone**: Select a time zone that applies to the start time you enter. If this time zone is different from the Grid time zone, the appliance converts the time you enter here based on the Grid time zone, after you save this schedule. When you display this schedule again, it displays the converted time. Selecting the time zone here does not affect any time zone settings in the Grid. (For information about setting the Grid and member time zones, see Managing Time Settings.)
   - **Admin Local Time**: Displays the Grid Master upgrade date and start time in the time zone of the administrator, as explained in Creating Local Admins.
   - In the upgrade member table, specify the following by clicking the corresponding field in each row:
     - **Group**: The name of the upgrade group. You can assign a different upgrade group by selecting the group from the drop-down list.
     - **Group Members**: When you expand an upgrade group, this field displays the group members.
   - **Warning**: This field turns yellow when there is a conflict among the upgrade groups. Hover your mouse over the field and the tooltip displays the member that contains the conflict. It also displays recommended upgrade groups in the Group column so you can change the group assignment to resolve the conflict. The tooltip can display one of the following: Grid Master Primary, DHCP Logging Member, or DHCP Failover. For information about how to resolve a conflict, see Resolving Upgrade Warnings. Select an upgrade group from the drop-down list in the Group column to assign a different upgrade group. Click Validate and Refresh to validate the new group assignment.
   - **Start Upgrade**: Specify when the upgrade occurs. Select one of the following from the drop-down list:
     - **Date/Time**: Select this to configure the upgrade start date, time, and time zone.
     - **After <group>**: Select After Grid Master to start the distribution immediately after the completion of the Grid Master distribution. Select an upgrade group that must complete its distribution before the group you are configuring. If you select this option, you cannot enter a date, time, and time zone.
2. Date, Time, and Time Zone are enabled only when you select Date/Time for Start Upgrade.
   - Date: Enter an upgrade start date in YYYY-MM-DD (year-month-day) format. You can click the calendar icon to select a date from the calendar widget.
   - Time: Enter an upgrade start time in hh:mm:ss AM/PM (hour:minute:second in AM or PM) format. You can select a time from the drop-down list.
   - Time Zone: By default, the appliance displays the time zone of the first Grid member in the Upgrade Group. You can change this time zone, if you want to enter the time using a different time zone. After you save the schedule though, the appliance converts the time you entered to the time zone of the upgrade group, if it is different. (For information about setting the Grid and member time zones, see Managing Time Settings.) To change the default time zone of an upgrade group, change the first group member in the Upgrade Group list, as explained in Adding Upgrade Groups.
   - Admin Local Time: Displays the data and time in the time zone of the administrator, as explained in Creating Local Ad mins.
   - Upgrade Members: Indicates whether the upgrade within the group occurs simultaneously or sequentially. You cannot edit this field here. You define this when you create the upgrade group. To change this setting, see Modifying Upgrade Groups.

3. Save the configuration.

The appliance does not save the schedule and displays an error message if the schedule contains the following:

- Circular dependencies between upgrade groups; for example, the upgrade of Group A is scheduled after Group B, and the upgrade of Group B is scheduled after Group A.
- The upgrade time is in the past.

The appliance also does not save the schedule and displays a warning when there is a group assignment conflict. For information about how to resolve these conflicts, see Resolving Upgrade Warnings. Otherwise, the appliance confirms that the schedule is saved and indicates whether the upgrade schedule is active.

Resolving Upgrade Warnings

The appliance can generate the following warnings when you schedule an upgrade:

- GMC: To resolve this warning, put all Grid Master candidates in the first upgrade group.
- DNS Primary: To resolve this warning, put all the members that are serving as DNS primaries in the first upgrade group.
- DHCP Logging Member: To resolve this warning, put the DHCP logging member in the first upgrade group.
- DHCP Failover: To resolve this warning, place the peers of a DHCP failover association in separate upgrade groups. Ensure that you schedule upgrades of the failover peers close to each other to minimize configuration rules. NIOS does not allow DHCP configuration changes that affect the communication between the peers until both peers are upgraded.

Upgrading Groups Immediately

After you schedule an upgrade with multiple upgrade groups, you can choose to immediately upgrade an upgrade group that has not been upgraded yet. This function is available only for scheduled upgrades.

To upgrade an upgrade group now:

1. From the Grid tab, select the Upgrade tab, and then click Toggle Group List View.
2. In the Group List view, click the Upgrade Group Now icon in the upgrade group row. Grid Manager immediately upgrades the selected group.

Upgrading a Single Member Immediately

After the Grid Master has been upgraded, you can choose to immediately upgrade a specific member that has not been upgraded yet. This function is available only for scheduled Grid upgrades from NIOS 6.4.0 to a later release. You can upgrade a single member only when the Grid upgrade is paused, and you cannot upgrade the Grid Master, reporting appliance, and an offline member. Once the member has been manually upgrades, the appliance skips this member when its scheduled upgrade time is reached.

To upgrade a specific member now:

1. From the Grid tab, select the Upgrade tab.
2. Pause the upgrade.
3. Click Toggle Member List View, and select the member check box from the table.
4. From the Toolbar, click Upgrade -> Upgrade Single Member. Grid Manager immediately upgrades the selected member.

Reverting a Single Member

During an upgrade from NIOS 6.4.0 to a later release, you can revert a specific member that has already been upgraded and is within its revert time window. The revert single member feature is useful when you want to troubleshoot issues, such as service outages, on a specific member after it has been upgraded. You can revert a member only when the Grid upgrade is paused, and you cannot revert the Grid Master, reporting appliance, and an offline member. If the upgrade is paused and you have reverted a member in an upgrade group that has already completed the upgrade, you must move the member to another upgrade group that has not been upgraded before you can proceed with the upgrade.
Once a member is upgraded, the appliance starts counting down and displays the time that is left for you to revert this member. You can revert the member before the revert time window expires. The default time window to revert a member is 24 hours. You can view the time that is left to revert the member in the Member List view, as described in Grid and Member Status. You can also use the CLI commands `set default_revert_window` to configure the default revert time window for the Grid. For information about this command, refer to the Infoblox CLI Guide. Once a member exits the revert time window, you must revert the entire Grid in order to revert the member.

**Note:** You may potentially lose some data when you revert a member. The appliance keeps information about DHCP leases and DNS records intact.

To revert a specific Grid member during a scheduled Grid upgrade:

1. From the Grid tab, select the Upgrade tab.
2. Pause the upgrade.
3. Click Toggle Member List View, and then select the member check box.
4. From the Toolbar, click Revert -> Revert Single Member.

Grid Manager displays a message indicating that the revert process disrupts Grid services. Read the message carefully, and then click Yes to confirm your decision to revert the member. Be aware that when you revert a member, some changes made since the member was last upgraded may get lost.

**Upgrade Process**

When an upgrade starts, Grid Manager checks if the nodes of an HA Grid Master have the same NIOS software version on their alternate partitions. If they do not have the same software version, the upgrade process stops. Grid Manager displays an error message and if it is a scheduled upgrade, Grid Manager deactivates the schedule as well. Otherwise, the upgrade process continues.

**Note:** During the upgrade, you can view the status of the Grid Master in the serial console.

During the upgrade, if a Grid member has not completed its distribution, it automatically resynchronizes with the Grid Master after the Grid Master upgrade is complete. Due to the nature of the upgrade sequence, HA pairs fail over during the upgrade. Therefore, be aware that the active and passive nodes reverse roles. The order in which Grid members upgrade, including when HA pairs fail over, is shown in Figure 10.1 (for an HA Grid Master) and Figure 10.2 (for a single Grid Master).

**Figure 10.1 Upgrade Sequence for an HA Grid Master and Grid Members**
Note: Grid members that do not have the correct NIOS version on their alternate partitions due to an incomplete distribution automatically resynchronize the NIOS version with the Grid Master, and then upgrade.

Figure 10.2 Upgrade Sequence for a Single Grid Master and Grid Members
The Grid Manager session terminates when the HA Grid Master fails over from Node 1 to Node 2, or when the single Grid Master reboots and goes offline. During a scheduled upgrade, the Grid members that have not upgraded yet can join the Grid and function normally until their scheduled upgrade time. When the upgrade finishes, the upgrade schedule is set to inactive.

Managing Upgrades

During an upgrade, Grid Manager displays a system message at the top of the screen indicating the Grid is being upgraded. After you start an upgrade, you can pause or resume it. For information, see Pausing and Resuming Upgrades and Monitoring Distribution and Upgrade Status.

Pausing and Resuming Upgrades

The following are some operational guidelines for performing an upgrade:

- You may not be able to perform certain administrative tasks during an upgrade.
- The Grid Manager session terminates when an HA Grid Master fails over from Node 1 to Node 2, or when a single Grid Master reboots and goes offline. You can log back in to the appliance after the upgrade.
- When you pause an upgrade, you can do the following
  - Change the sequence of the upgrade groups
  - Change the scheduled upgrade time for an upgrade group

To pause an upgrade, from the Grid Upgrade Status bar, click the Pause icon. When you pause an upgrade, Grid Manager displays a system message at the top of the screen indicating the upgrade is paused, until you resume the upgrade. For information about the upgrade status of each member, see Monitoring Distribution and Upgrade Status.

To resume an upgrade:

1. From the Grid Upgrade Status bar, click the Resume icon.
2. When the appliance displays a dialog box confirming that you want to resume the upgrade, click Yes to continue.

Members that have not completed or started upgrades that were scheduled at an earlier time resume the upgrade.

Monitoring Distribution and Upgrade Status
During a distribution or an upgrade, Grid Manager displays the status of the distribution or upgrade in the status bar. It also displays the process status for each member. You can view the status in either the Member List view or Group List view from the Grid tab -> Upgrade tab.

When you perform a distribution or an upgrade, the status bar displays the overall Grid distribution status with a progress bar that describes the process being performed. The status bar also displays the number of members that have completed the distribution or upgrade.

A difference between a distribution and an upgrade process is that during an upgrade, the Grid Manager session terminates when an HA Grid Master fails over from Node 1 to Node 2, or when a single Grid Master reboots and goes offline. You can log back in to the appliance after the upgrade.

**Grid and Member Status**

You can view the distribution and upgrade process status at the Grid and member level. To view the process status, from the Grid tab, select the Upgrade tab, and then click **Toggle Member List View**.

The status bar displays the status of the overall Grid process. It contains a progress bar that indicates the percentage of completion. It also shows the number of members that have completed the process.

Grid Manager displays the following information for each member:

- **Member**: The name of the Grid member.
- **Group**: The upgrade group to which the member belongs.
- **HA**: Indicates whether the member is an HA pair or not.
- **Status**: The current distribution or upgrade status. This can be Running (green) or Offline (red).
- **IPv4 Address**: The IPv4 address of the member.
- **IPv6 Address**: The IPv6 address of the member.
- **Running Version**: The NIOS software version that is currently running on the member.
- **Alternate Version**: Displays the NIOS software version to which the appliance can revert.
- **Distribution/Upgrade Status**: The current distribution or upgrade status. When the distribution or upgrade is in progress, Grid Manager displays a progress bar in this field to indicate the percentage of completion.
- **Hotfix**: The name of the hotfix that was last run on the member.
- **Status Time**: The date, time, and time zone of the status displayed.
- **Member Revert**: Indicates whether the member has been reverted or not. This appears only when the member has been upgraded from NIOS 6.4.0 to a later NIOS release.
- **Time to Revert**: The time (in HH:MM:SS format) left to revert a member. This appears only when the member has been upgraded from NIOS 6.4.0 to a later NIOS release.
- **Site**: The location to which the member belongs. This is one of the predefined extensible attributes. The appliance automatically refreshes the information in this panel.

**Upgrade Group Status**

You can view the distribution or upgrade status of an upgrade group in the group list view. In this view, the distribution or upgrade status rolls up to the group level. You can expand an upgrade group to view the status of individual member. However, you cannot view detailed status of a selected member from this view.

To view the process status of an upgrade group, from the Grid tab, select the Upgrade tab, and then click **Toggle Group List View**. Grid Manager displays the following information for each member in an upgrade group:

- **Group**: The upgrade group to which the member belongs.
- **Member**: The name of the Grid member.
- **Status**: The current member status. This can be Running (green) or Offline (red).
- **IPv4 Address**: The IPv4 address of the member appliance.
- **IPv6 Address**: The IPv6 address of the member appliance.
- **Running Version**: The NIOS software version that is currently running on the member.
- **Distribution Status**: The current distribution status. For an upgrade group, Grid Manager displays a progress bar to indicate the overall percentage of completion. For a member, Grid Manager displays the state of the distribution process.
- **Timestamp**: The date, time, and time zone of the status displayed.

**Detailed Status**

You can view detailed process information of a member during a distribution or an upgrade. To view detailed process information:

1. From the Grid tab, select the Upgrade tab, and then click **Toggle Member List View**.
2. Select a member and then click the Detailed Status icon.

Grid Manager displays a panel that shows the required steps during a distribution or an upgrade. It also displays a color indicator, next to each step, to indicate the current status of each step. The color indicator can be one of the following:

- **Grey**: The process has not started yet.
- **Green**: The process is complete.
- **Blue**: The distribution or upgrade that is in progress.
- **Red**: There is an error; Grid Manager displays a description of the problem.
- **Yellow**: A warning message.
When the selected member is an HA pair, Grid Manager displays the status information for both nodes. The panel remains open until you close it or select a different member.

Downgrading Software

Each Infoblox appliance model has a minimum required release of Infoblox software. Before downgrading an appliance, refer to the document, Minimum Required Release Software for Hardware Platforms, that shipped with your product. The downgrade procedure is for single independent appliances only. Infoblox does not support software downgrades for Grid members, but you can revert to the previous NIOS release (see the next section) on a Grid Master.

Caution: Although the downgrade process preserves license information and basic network settings, it does not preserve data. After you complete the downgrade procedure, all data in the database is lost.

To downgrade software on a single independent appliance running NIOS 4.0 or later:

1. From the Grid tab, select the Upgrade tab, and then click Downgrade from the Toolbar. Grid Manager displays a warning indicating that reverting to the current release is not possible once you start the downgrade. Read the warning carefully, and then click Yes to confirm your decision to downgrade.

2. In the Choose file dialog box, navigate to the downgrade image file, and then click Open to upload the file. The appliance uploads the file to the Grid Master. You cannot stop the downgrade process once you start it. Grid Manager displays the downgrade status in the status bar.

Reverting the Grid to the Previously Running Software

You can revert the Grid to a version of software that was previously running on your NIOS appliance. The NIOS appliance stores the previous software version in its backup software partition. You can see if there is a software version to which you can revert and its version number in the Alternate Version column in the Grid Version Information section of the Upgrade tab. To view the software version, from the Grid tab, select the Upgrade tab. Note that once you start distributing a new NIOS version after an upgrade, you cannot revert to a previous NIOS version.

Be aware that when you revert to this software, changes made since the Grid was last upgraded are lost, including the new DHCP leases and other DNS changes.

To revert to a version of software previously running on a Grid or on an independent appliance or HA pair:

From the Grid tab, select the Upgrade tab, and then click Revert -> Revert Grid from the Toolbar.

Grid Manager displays a warning indicating that the revert process disrupts Grid services. Read the warning carefully, and then click Yes to confirm your decision to revert.

Applying Hotfixes

Infoblox periodically releases hotfixes that contain resolved issues. Only superusers can apply hotfixes through Grid Manager. When you install hotfixes through Grid Manager, you can apply them to the Grid Master and All Grid members, the Grid Master only, the Grid Master and Grid Master Candidates, or selected Grid members. This feature is supported on appliances running NIOS version 7.1 or later. Note that each hotfix addresses specific issues. Infoblox recommends that you verify the hotfix before you apply it to ensure that it is the correct version.

After you apply a hotfix, Grid manager displays the hotfix status in the Upload Status bar. In addition, you can view the history of the most recent list of applied hotfixes in the Hotfix History dialog box. For information about viewing hotfix history, see Viewing Hotfix History.

Note: A hotfix installation may fail if there is a mismatch in the NIOS software versions or if a hotfix image fails to meet the software or hardware restrictions.

To apply a hotfix:

1. From the Grid tab, select the Upgrade tab, and then click Apply Hotfix from the Toolbar and select one of the following:
   - To Grid Master and all Grid Members: Click this to apply hotfix to the Grid Master and all Grid members.
   - To Grid Master: Click this to apply hotfix to the Grid Master only.
   - To Grid Master and Grid Master Candidates: Click this to apply hotfix only to the Grid Master and Grid Master candidates.
   - To selected Grid Members: Click this to apply hotfix to the selected Grid member. This option is available only after you have selected a Grid member or members.

2. In the Apply Hotfix dialog box, click Select and navigate to the hotfix image file you want to upload. Click Open to select the file, and click Upload.

Note: If you have already installed a hotfix and subsequently try to upgrade or downgrade NIOS, the appliance displays a warning message because resolved issues in the hotfix will no longer be valid if the upgrade or downgrade version does not contain the original hotfix.

The appliance applies the hotfix to the targeted appliance(s). You cannot stop the hotfix process once you start it. Grid Manager displays the hotfix status in the Upload Status bar.

Viewing Hotfix History

You can view hotfix history on selected members. To view the hotfix history:
1. From the Grid tab, select the Upgrade tab, click the Show Hotfix History icon in the Hotfix column.

2. The Hotfix History dialog box displays the following information:
   - **Date**: The timestamp when the hotfix was applied.
   - **Hotfix**: The name of the hotfix that was last run on the member. The name of the hotfix image file that was applied to the member.

3. Click Close to close the Hotfix History dialog box.

### Backing Up and Restoring Configuration Files

Infoblox recommends that you regularly back up your configuration files and/or discovery database files. You can back up your system files locally on the appliance or to your management system, or use TFTP (Trivial File Transfer Protocol), FTP (File Transfer Protocol), or SCP (Secure Copy) to back them up to a remote server. Backing up and restoring the configuration files using TFTP, FTP, or SCP is supported on both IPv4 and IPv6 communication protocols. You can select to back up files manually or schedule automatic backups for a later date.

To avoid missing a backup when a remote server is unavailable during a scheduled automatic backup, you can choose to save files locally on your appliance while backing up to the remote server. Both the local and remote backup files share the same date because NIOS saves these files from the same backup. The backup file is a .tar.gz file that contains the configuration settings, data set, and TFTP files. Note that the local backup contains only the Grid backup. It does not contain backups for reporting and Network Automation.

You may also schedule automatic backups of the discovery database, which consists of the complete discovery data for networks and network devices such as core, distribution and edge routers, enterprise switches, security devices, and end host devices. NIOS backs up the discovery database in a .tar.gz file, with the raw discovery data formatted as an XML file.

**Note:** Infoblox recommends that you backup the configuration after you convert a Grid to a different mode. Restoring the old backup by performing a forced restore, may prevent the Grid members from rejoining the Grid Master after the restore.

The following sections describe how to use the backup and restore functions:

- **Backing Up Files**
- **Automatically Backing Up Data Files**
- **Backing Up Files**
- **Restoring Backup Files**
- **Downloading Backup Files from a Different Appliance**

**Note:** Infoblox highly recommends that you always back up the current configuration file before upgrading, restoring, or reverting the software on the appliance. If you are performing these operations on appliances licensed for Discovery and that perform discovery, the discovery database can be backed up and restored using the same mechanisms.

### Backing Up Files

You can back up system files and discovery databases periodically and on demand. You can then restore the files on the same appliance or on a different appliance. For information about restoring files, see **Restoring Backup Files**. You can configure the appliance to automatically back up the files on a weekly, daily, or hourly basis.

Infoblox recommends that you back up the system files during off-hours to minimize the impact on network services. By default, the automatic backup function is turned off. You must log in with a superuser account to back up files.

You can back up system configuration and/or discovery database files to the following:

- A local directory
- The management system that you use to operate the appliance
- A TFTP server
- An FTP server. This option requires that you have a valid username and password on the server prior to backing up files.
- An SSH server that supports SCP. This option requires that you have a valid username and password on the server prior to backing up files.

### Local Backup

You can store a backup file on the appliance itself. However, Infoblox recommends that you store backup files in an alternate location. When you back up the system files locally, the appliance uses the following format to name the file: BACKUP_YYYY_MM_DD_MM.tar.gz. For example, a file name of BACKUP_2013_11_30_23_00 means that the file is backed up on November 30th, 2013 at 11:00 PM. The appliance can save up to 20 configuration files, regardless of how often the files are saved (weekly, hourly, or daily). Ensure that you take the size of the configuration file into consideration when backing up files because the storage limit on an appliance is 5 Gb (gigabytes). If your configuration file is 500 Mb (megabytes), then the appliance can store 10 configuration files. When uploading configuration files on to a TFTP, FTP, or SCP server, you must consider the file size on that server as well.

### Using TFTP

TFTP is a client-server protocol that uses UDP as its transport protocol. It does not provide authentication or encryption, therefore it does not require a username or password.
When you back up the system files to a TFTP server, you select the backup file you want to download, enter the name in which the file is stored on the TFTP server and the server IP address.

Using FTP

FTP is a client-server protocol used to exchange files over TCP-based networks. The appliance, as the FTP client, connects to a remote FTP server that you identify. When you use FTP to back up the system files, the password and file contents are transmitted in clear text and may be intercepted by other users. When you back up the system files to an FTP server, the appliance, as the FTP client, logs on to the FTP server. You must specify the username and password the appliance uses to log on to the FTP server. The user account must have write permission to the directory to which the appliance uploads the backup file.

Using SCP

SCP is more secure than TFTP and FTP. It uses the SSH protocol to provide authentication and security. You can use SCP to back up the NIOS system files to a server running SSHv2. When you use SCP to back up the system files to an SSH server, you must specify the username and password the appliance uses to log on to the server. Note that you must use either “password” or “Password” in the SCP password prompt because the appliance does not recognize “PASSWORD” in the prompt. Therefore, ensure that you customize the SCP password prompt to say “Enter your password” or “Enter your Password.” Otherwise, the SCP backup will fail. The user account must have write permission to the directory to which the appliance uploads the backup file. In addition, make sure that you enter the correct IP address of the SSH server; the appliance does not check the credentials of the SSH server to which it connects.

Note: The SCP protocol uses SSH for data transfer and thus provides the same authentication and security as SSH. SCP uses LAN1 regardless of whether the MGMT port is enabled or not.

Automatically Backing Up Data Files

Infoblox recommends that you regularly back up your configuration files and/or discovery database files. The easiest way to accomplish this task is to configure the appliance for scheduled automatic backups of the NIOS configuration files. When you automatically back up a configuration file on the appliance, the file is named in the format <GRIDNAME>_YYYY_MM_DD_HH.MM.tar.gz. The default time for an automatic backup is 3:00 AM. Infoblox recommends scheduling configuration file backups to take place during the slowest period of network activity. You can choose a schedule for when and how often files are backed up: weekly, daily, or hourly.

If a Grid has a discovery member, you may also schedule automatic backups of the Discovery database, which consists of the complete discovery data for networks and network devices such as core, distribution and edge routers, enterprise switches, security devices, and endpoint devices. NIOS backs up the Discovery database in a .tar.gz file, with the raw Discovery data formatted as an XML file. For information on discovery features and requirements, see the chapter Infoblox x Network Insight.

To automatically back up a database file on an independent appliance or Grid Master:

1. From the Grid tab, select the Grid Manager tab, and then click Backup -> Schedule Backup from the Toolbar.
2. In the Schedule Backup dialog box, select the destination of the backup file from the Backup to drop-down list:
   - **TFTP**: Back up system files to a TFTP server.
   - **Keep local copy**: Select this to also save a local copy of the backup file on your appliance. This is disabled by default. The local backup contains only the Grid backup, it does not contain backups for reporting and Network Automation. Note that when you select this, the total backup time will increase.
     - **IP Address of TFTP Server**: Enter the IP address of the TFTP server to which you want to back up the system files.
     - **Directory Path**: Enter the directory path of the file. For example, you can enter /archive/backups. The directory path cannot contain spaces. The folder or directory you enter here must already exist on the specified server. Do not include the file name in the directory path.
     - **Recurrence**: Select how often you want to back up the files. You can select Weekly, Daily, or Hourly from the drop-down list. When you select Weekly, complete the following:
       - **Every**: Choose a day of the week from the drop-down list.
       - **Time**: Enter a time in the hh:mm:ss AM/PM format. You can also click the clock icon and select a time from the drop-down list. The Grid Master creates a backup file on the selected day and time every week. When you select Daily, enter a time in the hh:mm:ss AM/PM format. You can also select a time from the drop-down list.
       - **Minutes after the Hour**: Enter the minute after the hour when the Grid Master creates a backup file. For example, enter 5 if you want the Grid Master to create a backup file five minutes after the hour every hour.
       - **Disable Scheduled Backup**: Select this if you want to disable automatic backups from occurring now. You can still save the settings for future use.
   - **FTP**: Back up system files to an FTP server.
   - **Keep local copy**: Select this to also save a local copy of the backup file on your appliance. This is disabled by default. The local backup contains only the Grid backup, it does not contain backups for reporting and Network Automation. Note that when you select this, the total backup time will increase.

select this, the total backup time will increase.

- **IP Address of FTP Server**: The IP address of the FTP server.
- **Directory Path**: Enter the directory path of the file. For example, you can enter `/archive/backups`. The directory path cannot contain spaces. The folder or directory you enter here must already exist on the specified server. Do not include the file name in the directory path.
- **Username**: Enter the username of your FTP account.

**Note**: If you have configured AD server for authentication, you must specify “domain name\username”.

- **Password**: Enter the password of your FTP account.
- **Recurrence**: Select how often the scheduled backups should occur. You can select **Weekly**, **Daily**, or **Hourly**. For information, see **TFTP**.
- **Disable Scheduled Backup**: Select this if you want to disable automatic backups from occurring now, but want to save the settings for future use.
- **SCP**: Back up system files to an SSH server that supports SCP.
- **Keep local copy**: Select this to also save a local copy of the backup file on your appliance. This is disabled by default. The local backup contains only the Grid backup, it does not contain backups for reporting and Network Automation. Note that when you select this, the total backup time will increase.
  - **IP Address of SCP Server**: The IP address of the SCP server.
  - **Directory Path**: Enter the directory path of the file. For example, you can enter `/archive/backups`. The directory path cannot contain spaces. The folder or directory you enter here must already exist on the specified server. Do not include the file name in the directory path.
  - **Username**: Enter the username of your SCP account.

**Note**: If you have configured AD server for authentication, you must specify “domain name\username”.

- **Password**: Enter the password of your SCP account.
- **Recurrence**: Select how often the scheduled backups should occur. You can select **Weekly**, **Daily**, or **Hourly**. For information, see the **TFTP** section.
- **Disable Scheduled Backup**: Select this if you want to disable automatic backups from occurring now. You can still save the settings for future use.

**Note**: When you select **FTP** or **SCP**, ensure that you have a valid username and password on the server prior to backing up the files.

- **Grid Master (Local)**: Back up to a local directory on the Grid Master. This is the default. By default, the Grid Master generates a backup file and saves it locally in its own storage at 3:00 AM daily. Be aware that backing up the Grid and saving it locally on an hourly basis increases the turnover of files stored on the Grid Master. Backing it up hourly to a remote server increases the overall amount of traffic on your network.
  3. If the Grid has a discovery member, Grid Manager displays the NIOS data and Discovery data check boxes. You can select the NIOS data check box, to back up NIOS configuration data for the Grid and select the Discovery data check box, to back up discovery data for the Grid.
  4. If the Grid has a reporting member, Grid Manager displays the Infoblox Splunk App check box. You can select the Infoblox Splunk App check box, to back up Splunk application reporting data.
  4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Manually Backing Up Data Files

You can manually back up a NIOS data file in addition to scheduling your backups. If a Grid has a discovery member, you can also manually back up the current discovery database. Doing so backs up the complete discovery database that is resident on the Consolidator appliance, which is a member of the Grid. Keep in mind that discovery processes may be taking place on the associated NIOS appliances licensed for that task. NIOS will temporarily suspend the Discovery service while the backup is being retrieved from the Consolidator appliance.

To back up manually:

1. From the Grid tab, select the Grid Manager tab, and then click **Backup -> Manual Backup** from the Toolbar.
2. In the Backup wizard, select the destination of the backup file from the Backup to drop-down list:
   - **My Computer**: Back up system files to a local directory on your computer. This is the default.
   - **TFTP**: Back up system files to a TFTP server.
     - **Filename**: Enter the directory path and the file name of the backup file. For example, you can enter `/archive/backups/Infoblox_2009_10_20_15_30`
     - **IP Address of TFTP Server**: Enter the IP address of the TFTP server to which you want to back up the system files.
   - **FTP**: Back up system files to an FTP server.
     - **Filename**: Enter the directory path and the file name of the backup file. For example, you can enter `/archive/backups/Infoblox_2009_10_20_15_30`
     - **IP Address of FTP Server**: The IP address of the FTP server.
     - **Username**: Enter the username of your FTP account.
     - **Password**: Enter the password of your FTP account.

**Note**: If you have configured AD server for authentication, you must specify “domain name\username”.
• SCP: Back up system files to an SSH server that supports SCP.
  • Filename: Enter the directory path and the file name of the backup file. For example, you can enter `/archive/backups/Infoblox_2009_10_20_15_30`.
  • IP Address of SCP Server: The IP address of the SCP server.
  • Username: Enter the username of your SCP account.

  Note: If you have configured AD server for authentication, you must specify "domain name/username".

  • Password: Enter the password of your SCP account.

  Note: When you select FTP or SCP, ensure that you have a valid username and password on the server prior to backing up the files.

3. If the Grid has a discovery member, Grid Manager displays the NIOS data and Discovery data check boxes. You can select the NIOS data check box, to back up NIOS configuration data for the Grid and select the Discovery data check box, to back up discovery data for the Grid.

   If the Grid has a reporting member, Grid Manager displays the Infoblox Splunk App check box. You can select the Infoblox Splunk App check box, to back up Splunk application reporting data.

4. Click Backup.

**Downloading Backup Files**

You can save an existing backup file, or create and save a new one to your local management system, a TFTP server, an FTP server, or a SCP server.

To download an existing backup file:

1. From the Grid tab, select the Grid Manager tab, and the click Backup -> Manage Local Backup from the Toolbar. Grid Manager displays the current backup files in the Manage Local Backups dialog box.

2. To download a backup file, select the check box of a backup file, and then click the Transfer icon. You cannot select multiple files for downloading.

3. Select one of the following from the Backup to drop-down list:

   • My Computer: Backup to a local directory on your computer. This is the default.
   • TFTP: Save the backup file to a TFTP server.
     • Filename: Enter the directory path and the file name of the backup file. For example, you can enter `/archive/backup/Infoblox_2009_10_20_15_30`.
     • IP Address of TFTP Server: Enter the IP address of the TFTP server to which you want to save the backup file.
   • FTP: Save the backup file to an FTP server.
     • Filename: Enter the directory path and the file name of the backup file. For example, you can enter `/archive/backup/Infoblox_2009_10_20_15_30`.
     • IP Address of FTP Server: The IP address of the FTP server.
     • Username: Enter the username of your FTP server account.
     • Password: Enter the password of your FTP server account.
   • SCP: Save the backup file to an SSH server that supports SCP.
     • Filename: Enter the directory path and the file name of the backup file. For example, you can enter `/archive/backup/Infoblox_2009_10_20_15_30`.
     • IP Address of SCP Server: The IP address of the SCP server.
     • Username: Enter the username of your SCP server account.
     • Password: Enter the password of your SCP server account.

  Note: When you select FTP or SCP, ensure that you have a valid username and password on the server prior to backing up the files.

4. Click Transfer Copy.

**Restoring Backup Files**

You can restore a backup file of a NIOS configuration or a Discovery database to an appliance running the same NIOS version as that of the appliance from which the backup file originates. You can also restore a backup file from an appliance running a NIOS version to an appliance running a later NIOS version as long as the upgrade from the earlier NIOS version to the later version is supported. For example, you can restore a backup file from an appliance running NIOS 6.10.0 to an appliance running NIOS 7.3.200 because upgrading from NIOS 6.10.0 to 7.3.200 is supported. However, you cannot restore a backup file from an appliance running NIOS 6.9.0 to an appliance running NIOS 7.3.200 because upgrading from NIOS 6.9.0 to 7.3.200 is not supported.

You can restore an existing backup file on the appliance from which it originates, or restore a backup file from a different appliance (referred to as a forced restore). To download a backup file from a different appliance, see [Downloading Backup Files from a Different Appliance](#). You must log in with a superuser account to back up and restore files. NIOS provides three ways to restore a backup file:

- From a local directory or the management system you use to operate the appliance
- From a TFTP server
From a remote server using FTP. This option requires that you have a valid username and password on the FTP server prior to performing a backup or restore.

**Note:** When you restore NIC interfaces to a VM, ensure that you provision appropriate NIC interfaces with the database content that must be restored to avoid any errors.

To restore a backup file to the same independent appliance or Grid Master:

1. From the **Grid** tab, select the **Grid Manager** tab, and then click **Restore** from the Toolbar.
2. In the **Restore** dialog box, choose one of the following from the **Restore from** drop-down list:
   - **My Computer:** Restore a file from your local computer. This is the default.
   - **Filename:** Click **Select File** to navigate to the configuration file.
   - **TFTP:** Restore a file from a TFTP server.
     - **Filename:** Enter the directory path and the file name you want to restore. For example, you can enter `/archive/backups/Infoblox_2009_10_20_15_30`.
   - **IP Address of TFTP Server:** Enter the IP address of the TFTP server from which you restore the configuration file.
   - **FTP:** Restore a file from an FTP server.
     - **Filename:** Enter the directory path and the file name of the backup file. For example, you can enter `/archive/backups/Infoblox_2009_10_20_15_30`.
     - **IP Address of FTP Server:** The IP address of the FTP server.
   - **Username:** Enter the username of your FTP server account.
   - **Password:** Enter the password of your FTP server account.
   - **Grid Master (Local):** Restore from a local directory on the Grid Master. In the **Backup Set** table, select the file you want to restore.
3. To restore NIOS configuration data, select the **NIOS data** check box.
4. To restore Discovery data, select the **Discovery data** check box. Discovery data should be restored to Consolidator appliances with the correct licensing.
5. To download a backup file from one appliance to a different appliance, select **Force Restore from Different Grid** to enable the feature, and then select one of the following:
   - **Retain Current Grid Master IP Settings** (this is the default)
   - **Overwrite Grid Master IP Settings**
6. Click **Restore.** In the **Confirm Restore** dialog box, click **Yes.**
   After restoring the file, the appliance restarts. The restore process overwrites all existing data. All pending scheduled tasks are not restored or reverted.
7. Close your current browser window, wait a few minutes, and then reconnect to the NIOS appliance.

### Downloading Backup Files from a Different Appliance

When you "force restore" a NIOS appliance, you download a backup file from one appliance to a different appliance. To restore a backup file to the same appliance or Grid Master, use the Restore function as described in **Restoring Backup Files.**

To download a backup file from one appliance to a different appliance:

1. From the **Grid** tab, select the **Grid Manager** tab, and then click **Restore** from the Toolbar.
2. In the **Restore** wizard, do the following:
   - **Restore from:** Choose a source from which you restore the configuration file, as described in **Restoring Backup Files.**
3. Select **Force Restore from Different Grid** to enable the feature, and then select one of the following:
   - **Retain Current Grid Master IP Settings** (this is the default)
   - **Overwrite Grid Master IP Settings**
4. Click **Restore.** In the **Confirm Restore** dialog box, click **Yes.**
   After restoring the file, the appliance reboots. The restore process overwrites all existing data. All pending scheduled tasks are not restored or reverted.
5. Close your current browser window, wait a few minutes, and then reconnect to the NIOS appliance.

### Using Database Snapshots

Infoblox recommends that you regularly create database snapshots that helps in mitigating the impact of any user errors in the NIOS configuration. Whenever there is an error in the NIOS configuration, you can roll back the database (onedb) to the snapshot that you have created earlier. This is potentially faster than restoring the database using the backup file.

The following sections describe how to create snapshots and roll back snapshots:

- **Creating Database Snapshots**
- **Rolling Back Database Snapshots**

#### Creating Database Snapshots

You can create a database snapshot periodically and save it locally on the appliance. You can create only one copy of the database snapshot at any given time. Each time you create a new snapshot, it overrides the previous snapshot. When you create a database snapshot, only data that is currently saved in the database is included in the snapshot. Only superusers are allowed to create a database snapshot. Creating database snapshots does not have any impact on the scheduled local backup. The snapshot saved locally on the appliance will not be affected if an HA failover occurs, but the snapshot is deleted during a Grid Master Candidate promotion, upgrade, downgrade, or if you restore the appliance using the backup file. Note that creating a database snapshot fails when any of the following operations are in progress:
Rolling Back Database Snapshots

If you have already created a snapshot, you can roll back the database to the snapshot to recover from any user errors in the NIOS configuration. Rolling back the database (onedb) to the snapshot is potentially faster than restoring the database from a backup file. Rolling back to the snapshot changes only the database, not any other transient data, such as file distribution, reporting splunk, discovery data, etc. Note that you might lose the data that you have saved after creating the snapshot. Only superusers can perform the rollback operation.

To roll back the database to the snapshot:

1. From the Grid tab -> Grid Manager tab, click Snapshot -> Rollback from the Toolbar.
2. The Rollback Snapshot dialog box displays the following information:
   - Snapshot Time: The date and timestamp when the snapshot was created.
   - Comment: Information about the snapshot.
3. Click OK.

Downloading Support Bundles

When you need assistance troubleshooting a NIOS appliance, you can log in to the appliance as a superuser, download the support bundle of the appliance, and then send it to Infoblox Technical Support for analysis. A support bundle is a tar.gz file that contains configuration files and the appliance system files. You can download a support bundle for an independent appliance and for each member in a Grid. When you download a support bundle for an HA pair, it includes the files of both nodes in the HA pair.

By default, the appliance includes the following files in the support bundle: core files, current logs, and rotated logs. Because core files can be quite large and take a significant amount of time to download, Infoblox recommends that you include core files in the support bundle only when requested by Infoblox Technical Support. You can include all the core files or specific core files in the support bundle when Infoblox Support requests them. Note that the option of downloading only specific core files is supported on appliances running NIOS version 8.0 or later. If your appliance supports multiple primary servers for DNS authoritative zones, you can select to include cached zone data in the support bundle. This data is not included in the bundle by default.

To download a support bundle:

1. From the Grid tab, select a member check box, and then click Download -> Support Bundle from the Toolbar.
2. In the Download Support Bundle dialog box, select the files you want to include in the support bundle, and then click OK:
   - Core Files: Infoblox recommends that you include these files only when requested by Infoblox Technical Support.
   - Current Logs: Infoblox recommends that you always include these files in the support bundle.
   - Rotated Logs: These are rotated logs that contain historical information.
   - Cached DNS Recursive Data: Select this to include cached DNS recursive data in the support bundle. This is deselected by default.
   - Cached Zone Data: Select this to include cached DNS zone data in the support bundle. This is deselected by default.
   - Cloud Discovery Data: Select this to include cloud discovery data in the support bundle. This is deselected by default.
   - Files from the previously installed NIOS version: Select this to include files from the previously installed NIOS version in the support bundle. This is deselected by default.
   - Discovery SNMP Logs: Event logs related to device discovery SNMP probes of routers, switches and other network infrastructure devices.
   - Core Files: Infoblox recommends that you include these files only when requested by Infoblox Technical Support.
     - All Core Files: Select this to include all core files in the support bundle.
     - Select Core Files: Select this to include only specific core files in the support bundle. Click the Add icon in the table. Grid Manager displays the Core Files Selector dialog box from which you can select specific core files. You can delete a core file by selecting its check box and clicking the Delete icon. Note that on an HA pair, you can select the core files of the active node only.
3. Navigate to the location you want to save the file and change the file name. Do not change the .tar.gz file extension in the file name.
4. Send this file to Infoblox Technical Support.

Chapter 11 bloxTools Environment

The bloxTools environment provides a pre-installed environment for hosting custom web-based applications. This chapter includes the following sections:

- About the bloxTools Environment
- System Requirements
The bloxTools environment provides tools for creating custom applications that facilitate the administrative tasks in your organization. It provides a pre-installed environment for running applications using Perl, Python, PHP, CGI scripting, and Infoblox API libraries. Note that no direct external remote user (telnet and ssh, for example) or shell access is available in this environment.

The bloxTools environment "borrows" resources such as CPU, memory, disk space, and networking from the host Infoblox appliance, but is logically separated from the NIOS. The logical separation ensures that any failure in the bloxTools service does not affect the other services running on the appliance.

The bloxTools environment can only be configured to run on an independent appliance or a Grid member. You cannot run the bloxTools service on a Grid Master or a Grid Master candidate.

Note: In previous NIOS releases, you could run the bloxTools service only on a Grid Master. If bloxTools has been configured to run on a Grid Master before an upgrade, the bloxTools service continues to run on the Grid Master after an upgrade. This configuration is preserved mainly for migration purposes only. Infoblox strongly recommends that you move the bloxTools service to a Grid member after the upgrade. For information, see Moving the bloxTools Service.

In a Grid, you can run the bloxTools service only on one Grid member at a time, and you cannot configure this member as a Grid Master candidate. However, you can move the bloxTools service from one member to another. For information, see Moving the bloxTools Service.

On an HA member, the bloxTools service runs on the active node. If there is an HA failover, the bloxTools service is automatically launched after the passive node becomes active. For information, see About HA Pairs.

Note: When you run the bloxTools service on an independent appliance or a Grid member, the performance of other services running on the appliance may be affected. Infoblox recommends that you run the bloxTools environment on a member that does not host critical services.

After you enable the bloxTools service and configure its built-in file transfer services, you can upload content to the bloxTools portal using either an FTP (File Transfer Protocol) or SFTP (SSH File Transfer Protocol) client. The uploaded content is included in system backups and you can restore it from the backups.

If you have further questions about bloxTools, visit the community site at https://community.infoblox.com.

System Requirements

The following table shows which Infoblox physical appliances support the bloxTools service.

<table>
<thead>
<tr>
<th>Supported Infoblox Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>TE-810</td>
</tr>
<tr>
<td>TE-815</td>
</tr>
<tr>
<td>TE-1410</td>
</tr>
<tr>
<td>TE-1415</td>
</tr>
<tr>
<td>TE-2210</td>
</tr>
<tr>
<td>TE-2215</td>
</tr>
</tbody>
</table>

The following table shows which Infoblox appliances support the bloxTools service and the memory requirement for each. The service "borrows" host resources such as CPU, memory, and disk space from the host Infoblox appliance.

<table>
<thead>
<tr>
<th>Supported Infoblox Appliance</th>
<th>Memory Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>IB-V1410</td>
<td>128 MB to 2048 MB</td>
</tr>
<tr>
<td>IB-V1415</td>
<td>The default is 256 MB</td>
</tr>
<tr>
<td>IB-V1420</td>
<td></td>
</tr>
<tr>
<td>IB-V1425</td>
<td></td>
</tr>
<tr>
<td>IB-V2210</td>
<td>128 MB to 2048 MB</td>
</tr>
<tr>
<td>IB-V2215</td>
<td>The default is 256 MB</td>
</tr>
<tr>
<td>IB-V2220</td>
<td></td>
</tr>
<tr>
<td>IB-V2225</td>
<td></td>
</tr>
</tbody>
</table>
### Using the bloxTools Environment

Complete the following tasks to upload custom applications to the bloxTools environment:

1. Log in to the appliance as a superuser and configure the bloxTools service, as described in *Configuring the Service*.
2. Use an FTP or a SFTP client to upload content to the bloxTools environment.

In addition, you can schedule tasks as described in *Scheduling Tasks*, and monitor the bloxTools service as described in *Monitoring the Service*.

**WARNING:** Resetting the Grid member using either the reset all or reset database CLI commands permanently deletes the content you uploaded to the bloxTools environment. Infoblox recommends that you backup the appliance before using any of these commands.

### Configuring the Service

When you configure the bloxTools service, you can enable FTP, SFTP, and HTTPS, and set their operational parameters. FTP and SFTP are the services you use to upload data. You can disable these services when they are not in use. HTTPS must remain enabled to allow the web based bloxTools applications to run. Note that the bloxTools service uses the same SSL certificate as the host Infoblox appliance. For information on certificates, see *Managing Certificates*.

You can configure the bloxTools service on port 443, 444 or on a port between 1024 to 63999. You can also enable HTTP to HTTPS redirection for the bloxTools service from the default HTTP port 80 to any specified HTTPS port. When you enable HTTP to HTTPS redirection, all the requests sent to the HTTP port are redirected to the HTTPS port configured for the bloxTools service. By default, NIOS appliance does not redirect HTTP requests to HTTPS.

**Note:** When you redirect HTTP to HTTPS, the connection is not as secure as compared to connecting directly through HTTPS.

Note the following when you configure the bloxTools service on port 443:

- HTTP to HTTPS redirection from Grid member to Grid Master is disabled.
- HTTP file distribution service is not allowed.

In previous NIOS releases, you could run the bloxTools service on a Grid Master or a Grid Master candidate. If you have not removed the bloxTools service from a member before you upgrade it to NIOS 6.11.0 or later, you cannot configure the bloxTools service on port 443 until you move the bloxTools service to an upgraded Grid member. For information, see *Moving the bloxTools Service*.

To configure the bloxTools service:

1. Log in as a superuser.
2. From the Grid tab, select the Grid Manager tab, and then click **bloxTools**. In the Services tab, click Edit -> Grid bloxTools Properties from the Toolbar.
3. In the Grid bloxTools Properties editor, complete the following:
   - **Enable Web Service**: Select HTTPS Port to enable users to access the applications through an HTTPS connection. The default port is 444. You can change the default HTTPS port to 443 or to a port between 1024 to 63999.
   - **Redirect Bloxtools HTTP to HTTPS**: Select this check box to enable redirection from the default HTTP port to the HTTPS port. The default HTTP port is 80. This is disabled by default.
   - **Enable FTP Service**: Select FTP Port to enable the FTP service. The default port is 26. You can change the port number to suit your environment.
   - **Enable SFTP Service**: Select SFTP Port to enable the SFTP service for secure file transfer. The default port is 28. You can change the port to a number between 1024 and 63999, provided that the port is not currently used for another purpose.
   - **Login**: Enter the username for the FTP and SFTP services. The username can contain lower case letters, numbers, underscores (_), and dollar signs ($), and it must begin with a letter, not a number.
   - **Set Password**: Enter the password for the FTP and SFTP services in this field.
   - **Retype Password**: Enter the same password.

   **Note:** The password is sent as clear text when you use the FTP service. To maintain security on the Infoblox appliance, this password should be different from the password set for the Infoblox appliance.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

When you configure the bloxTools service on an independent appliance, you can configure the allocated memory in the System bloxTools Properties editor. For information, see *Allocating Memory*.

### Allocating Memory

<table>
<thead>
<tr>
<th>IB-V4010</th>
<th>128 MB to 4096 MB</th>
</tr>
</thead>
<tbody>
<tr>
<td>IB-V4015</td>
<td></td>
</tr>
<tr>
<td>IB-V4020</td>
<td></td>
</tr>
<tr>
<td>IB-V4025</td>
<td></td>
</tr>
</tbody>
</table>

The default is 256 MB
You can configure the memory you want to allocate to the bloxTools service. You must configure this at the member level. If you run the bloxTools service on an independent appliance, you can configure the allocated memory in the System bloxTools Properties editor.

To configure the allocated memory:

1. Log in as a superuser.
2. From the Grid tab, select the GridManager tab, and then click bloxTools. In the Services tab, click Edit -> MemberbloxToolsProperties from the Toolbar.
3. In the MemberbloxToolsProperties editor, complete the following:
   - **Allocated Memory (MB):** The service “borrows” host resources such as CPU, memory, and disk space from the host Infoblox appliance. The default amount of memory the appliance allocates for the bloxTools environment is 256 MB. You can change this allocation, depending on the appliance platform. See System Requirements for the requirements and allowed values of each appliance.

Uploading Files

Use an FTP or a SFTP client to upload content, such as Perl modules, JavaScript files, PHP files, CGI files, and image files, to the bloxTools environment. You can upload a maximum of 4 GB of data. After you have uploaded content to your bloxTools environment, you should disable the FTP and SFTP services to prevent unauthorized or accidental changes.

To upload files using the FTP service:

1. Open an Internet browser window and log in to the FTP service by entering:
   
   ftp://Grid_member_ip_addr:ftp_port
   
   For example, if the IP address of the Grid member is 10.1.1.1 and the FTP port number is 26, enter: ftp://10.1.1.1:26
2. In the Authentication Required dialog box, enter the username and password. This is the username and password you entered for the FTP service in the bloxTools Environment editor on the appliance.
3. Follow the instructions provided by your FTP client to upload the files.

To upload files using the SFTP service:

1. Open a terminal window and log in to the SFTP service by entering:
   
   sftp -oPort=sftp_port sftp_user@Grid_member_ip_addr
   
   For example, if the IP address of the Grid member is 10.1.1.1, the login username for the SFTP service is jdoe, and the SFTP port number is 28, enter:
   
   sftp -oPort=28 jdoe@10.1.1.1
2. Enter the password. This is the password you entered for the SFTP service in the bloxTools Environment editor on the appliance.
3. Follow the instructions provided by your SFTP client to upload the files.

**Note:** On a computer running Microsoft Windows, you can use WinSCP as the FTP or SFTP client for uploading files. The bloxTools environment stores the uploaded data in the /portal directory.

Scheduling Tasks

bloxTools includes support for the Perl module Config::Crontab so you can manage scheduler services. You can use the scheduler to execute commands in the future. You can also schedule recurring commands. For example, you can schedule the creation of a host record or schedule recurring reports. The scheduler allows default "user level" crontab access and you can use the user account 'nobody' to submit commands. The Grid Master replicates the crontab data to the Master Candidates.

Moving the bloxTools Service

In a Grid, you can move the bloxTools service from one Grid member to another. When you move the bloxTools service, the source member synchronizes data with the Grid Master, and the Grid Master synchronizes data with the destination member. The time to resynchronize the bloxTools data on to the destination member depends on the amount of data to synchronize and the Grid configuration. If the migration takes longer than two minutes, it becomes a long running task. This allows the move of the bloxTools service to run in the background while you perform other tasks. For information, see About Tasks. Note that on an independent appliance, you cannot move the bloxTools service to another member.

After an upgrade from previous NIOS releases, Grid Manager displays a warning message in the system message panel if you have previously configured to run the bloxTools service on the Grid Master. You can click Move in this panel to launch the Move bloxTools dialog box to move the bloxTools service to a Grid member.

To move the bloxTools Service:

1. From the Grid tab, select the Grid Manager tab -> Members tab, and then click bloxTools -> Move from the Toolbar.
2. In the Move bloxTools dialog box, complete the following:
   - **Source Member:** Displays the name of the Grid member that is currently running the bloxTools service. You cannot modify this field.
   - **Destination Member:** Click Select. In the Member Selector dialog box, select the member to which you want to move the bloxTools service. Grid Manager displays the name of the selected member here.
3. Click Move.
The appliance synchronizes data with the Grid Master, and the Grid Master synchronizes data with the destination member. This may take a while to complete depending on your Grid configuration and the amount of data.

**Monitoring the Service**

Infoblox provides several tools for monitoring the bloxTools Environment. The bloxTools Environment has its own syslog service which you can access to view logs generated by the bloxTools service and its processes. The Detailed Status panel also displays the status of the bloxTools Environment.

**Viewing the Logs**

The bloxTools Environment generates the following logs:

- access.log: The Apache access log
- error.log: The Apache error log
- syslog.log: The bloxTools Environment system log

These log files are included in the support bundle. You can download the log files using FTP. You can also connect to the CLI of the member running the bloxTools environment and use the following commands to view the logs:

- Use the `show file` command to view the list of log files.
- Use the `show bloxtools` command to view the status of the bloxTools Environment.
- Use the `show file bloxtools portal_access` command to view the web portal access log.
- Use the `show file bloxtools portal_error` command to view the web portal error log.
- Use the `show file bloxtools portal_log` command to view the web portal system log.

**Viewing Detailed Status**

You can view the status of the bloxTools Environment from the Services tab of the Grid Manager tab. To display the bloxTools service status, from the Grid tab, select the Grid Manager tab -> Services tab, and then click bloxTools. Grid Manager displays all Grid members that can host the bloxTools service. The name of the Grid Master is displayed only if you have completed an upgrade and previously configured the bloxTools service to run on the Grid Master. Though you can continue to run the bloxTools service on the Grid Master, Infoblox strongly recommends that you move the bloxTools service to a Grid member. For information, see Moving the bloxTools Service.

Grid Manager displays the following information about all Grid members:

- **Name**: The Grid member name.
- **Service Status**: Indicates the current operational status of the bloxTools service running on the member. This can include the migration status if you are moving the bloxTools service to another member.
- **IP Address**: The IP address of the member.
- **Comment**: Information about the bloxTools Environment.
- **Sit**: The location to which the member belongs. This is one of the predefined extensible attributes.

The service status icon indicates the operational status of the bloxTools Environment and the usage percentages for the CPU, memory and disk resources. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gray</td>
<td>The bloxTools Environment is disabled or offline.</td>
<td></td>
</tr>
<tr>
<td>Green</td>
<td>The CPU, memory, and disk usage is below 80%.</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>Usage of at least one of the following resources is greater than or equal to 80%; CPU, memory or disk. The description indicates the percentage of each resource.</td>
<td></td>
</tr>
<tr>
<td>Red</td>
<td>The bloxTools Environment is down, or an essential service within the bloxTools Environment has failed.</td>
<td></td>
</tr>
</tbody>
</table>

**Chapter 12 RIR Registration Updates**

This chapter explains how to configure the Infoblox Grid to manage RIR (Regional Internet Registries) allocated addresses and submit registration updates to the RIPE database. It includes the following sections:

- RIR Address Allocation and Registration Updates
- About the RIPE Database
- Configuring RIR Registration Updates
  - Requirements and Permissions
  - Enabling Support for RIR Registration Updates
  - Configuring RIR Communication Settings
- Managing RIR Data
  - Adding RIR Organizations
**RIR Address Allocation and Registration Updates**

You can configure the Infoblox Grid to manage allocated IP address blocks that ISPs (Internet Service Providers) receive from their RIRs (Regional Internet Registries). An RIR is an entity that manages the Internet number resources, which include IP addresses and autonomous system numbers, within a specific region of the world. RIRs use SWIP (Share WHOIS Project) or RWhois (Referral WHOIS) servers to provide address allocation information for IP address blocks. Typically, an RIR determines the address blocks to be allocated for specific organizations (typically ISPs), while an ISP manages the allocated address blocks, associated organizations and corresponding RIR registrations. An organization can determine when to request for more address blocks from its RIR. Most ISPs manage multiple organizations and synchronize network address data with their RIRs every few months.

To leverage IPAM (IP Address Management) on the NIOS appliance, you can enable the Infoblox Grid to manage RIR allocated addresses and send registration updates to the RIPE (Réseaux IP Européens) database as often as you update RIR data on NIOS. RIPE is one of the five RIRs in the world that manages the allocation and registration of Internet number resources for Europe, Russia, the Middle East, and Central Asia.

**About the RIPE Database**

The RIPE database contains registration details of IP addresses and AS numbers originally allocated by the RIPE NCC (RIPE Network Coordination Center). The database contains information such as organizations that hold IP resources, where the allocations were made, and contact details for the networks. Organizations or individuals that hold the allocated address blocks are responsible for updating information in the database.

The NIOS appliance supports submitting registration and reassignment updates to the RIPE database, which can be accessed through the RIPE API interface or an email template. For more information, see Configuring RIR Communication Settings.

**Requirements and Permissions**

To manage RIR allocated addresses, organizations, and network utilization that contain RIR assignments, you must first enable support for RIR registration updates, and then configure the RIR communication method. Note that once you have enabled support for RIR registration updates, settings and fields that are relevant to this feature are enabled in Grid Manager. You do not need a special license to use this feature. Only superusers can create, modify, and delete RIR organizations. Limited-access users can manage RIR allocated address blocks if they have the required permissions to the objects.

To view and manage RIR related data, admins must have permissions to the applicable resources. For example, to view RIR networks, admins must have read-only permission to the networks; and to edit them, admins must have read/write permission to them. For more information about admin permissions, see About Administrative Permissions.

**Configuring RIR Registration Updates**

To manage RIR allocated addresses and send registration updates through NIOS, you first add RIR organizations and create RIR allocated networks in NIOS. You can then reassign network addresses within the RIR allocated address block to other organizations based on your requirements, and then configure NIOS to send registration updates directly to the RIPE database. Any data you manage through the Grid is handled by the Grid Master.

When the Grid Master is an HA pair, the active node handles the submission of data. If an HA failover occurs during a submission, the failing node immediately aborts the submission. The new active node resumes the next submission. For information about HA pairs, see About HA Pairs.

To manage and submit updates to the RIPE database, you must first enable the Grid to support RIR registration updates. You can then enter RIR information, such as RIR organizations and RIR attributes.

To configure the Grid to manage RIR allocated addresses and submit updates to RIPE, complete the following:

1. Enable support for RIR registration updates, as described in Enabling Support for RIR Registration Updates.
2. Define the method to communicate updates to RIPE, as described in Configuring RIR Communication Settings.
3. Add and configure RIR organizations and RIR organizational attributes, as described in Adding RIR Organizations.
4. Add allocated address blocks and assign specific network addresses to RIR organizations, as described in Adding and Assigning RIR Networks.
5. Review and submit registration updates to RIPE, as described in Previewing Registration Updates. You can also perform the following tasks:
   - View a list of RIR organizations, as described in Viewing RIR Organizations.

**Note:** The RIR registration update feature is not supported in a Multi-Grid configuration.
Enabling Support for RIR Registration Updates

Before you can manage RIR data through Grid Manager, you must first enable support for RIR registration updates. To enable support for RIR registration updates:

1. From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the General tab -> Advanced tab, and complete the following:
   - **Enable Updates of RIR Registrations**: Select this to enable the support for submitting RIR registration updates to the RIPE database. When you enable this feature, you can configure the appliance to send registration updates to RIPE for network reassignments and reallocations.
   
   **Note**: Ensure that you configure DNS resolvers for the Grid when you enable this feature. For information about how to configure DNS resolvers, see Enabling DNS Resolution.

3. Save the configuration.

Configuring RIR Communication Settings

You can configure the appliance to send RIR address updates to RIPE through the RIPE REST API or through an email using the maintainer email address specified in the RIR organization. Note that when you use the API method to delete a registered address block, you do not need to submit RIR attributes that match the data in the RIPE database. However, when you use the email method, you must enter RIR attribute values that match the data in the database. Otherwise, your submission will fail. To view examples of registration updates that NIOS sends, see Previewing Registration Updates.

To configure the RIR communication settings:

1. From the Administration tab, select the RIR tab, and then select RIR Settings -> RIPE from the Toolbar.
2. In the RIR Communication Settings - RIPE editor, select one of the following to determine how the appliance sends updates to RIPE. The default is API.
   - **API**: The appliance sends RIR updates to RIPE through the RIPE API. The default destination is https://rest.db.ripe.net for accessing the production database and https://rest-test.db.ripe.net for accessing the test database. Click Override and enter a different URL to override the default value. When you select this as the communication method, the registration status will be updated automatically after the registration update is completed. Note that RIPE supports only secure connections using HTTPS.
   - **Email**: The appliance sends RIR updates to RIPE through the email address displayed in the field. The default is auto-dbm@ripe.net. Click Override and enter a different email address to override the default value. The appliance uses a special email template that includes values of certain RIR attributes. If any of the RIR attribute values do not match the database in the RIPE database, your submission will fail. When you select Email as the communication method, ensure that you enable email notifications at the Grid level. For information how to enable email notifications, see Setting SNMP and Email Notifications. Note that when you select this as the communication method, the registration status will not be automatically updated. You can manually change the status. For information, see Modifying RIR Network Data.
   - **None**: The appliance does not send RIR updates to RIPE.

3. Save the configuration.

Managing RIR Data

An RIR organization provides information about an entity that has registered a network resource in the RIPE Database. This entity can be a company (such as an ISP), a nonprofit group, or an individual. You can add RIR organizations defined in the RIPE database and start managing their data through NIOS. After you have enabled support for RIR updates and configure the desired communication method for the updates, you can do the following to manage RIR data:

- Add RIR organizations and their associated data, as described in Adding RIR Organizations.
- Add the RIR allocated addresses to NIOS and assign specific address blocks to ISP organizations, as described in Adding and Assigning RIR Networks.
- View a list of organization objects, as described in Viewing RIR Organizations.
- Review the reassignment information before sending the updates to RIPE, as described in Previewing Registration Updates.
- Modify RIR organizational data and attributes, as described in Modifying RIR Organizations.
- Modify RIR network data and attributes, as described in Modifying RIR Network Data.
- Delete RIR organizations, as described in Deleting RIR Organizations.
- Delete delegated addresses from an organization, as described in Deleting RIR Networks.

Adding RIR Organizations

Before you can submit any RIR updates to the RIPE database, you must first add the RIR organization and its corresponding data to NIOS. You can also create additional organizations for ISP customers.

To add an organization:
1. From the Administration tab, select the RIR tab, and then click Add -> RIPE Organization.
2. In the Add RIPE Organization wizard, complete the following:
   - **Internet Registry**: The default is RIPE. This is the RIR that allocates address blocks to your organization. You cannot change this.
   - **Organization Name**: Enter the name of the organization that holds the resources allocated by RIPE NCC. You can enter up to 256 characters. Enter the name in this format: A list of words separated by white space. A word can be made up of letters, digits, the character underscore "_", and the character hyphen "-". The first character of a word must be a letter or digit and the last character of a word must be a letter, digit or a period. For example, you can enter SPRINT REGION.
   - **Organization ID**: Enter the handle or ID of the organization. You can enter up to 23 characters. Enter the ID in this format: Start with ORG- followed by two to four characters, then followed by up to five digits and a source specification. Note that the first digit cannot be "0". The source specification starts with "*" followed by the source name that contains up to nine characters in length. For example, you can enter ORG-CAL1-RIPE or ORG-CB2-TEST.
   - **Maintainer**: Enter the name of the maintainer for this organization. This is required. You can enter up to 256 characters; however, note that the RIPE database has an 80 characters limit for this field. A maintainer is any registrant or person to whom the authority to update has been delegated by another registrant either directly or indirectly, and who holds an identifier that allows updates to be authenticated and authorized. Data entered here must match exactly how the maintainer appears in RIPE.
   - **Password**: Enter the maintainer password. This is required. You can enter up to 256 characters.
   - **Retype Password**: Enter the same password.
   - **Organization**: Enter the name of the organization that holds the resources allocated by RIPE NCC. You can enter up to 256 characters.
   - **Email**: Enter the originating or source email address of the maintainer. This is required.
   - **ID**: Enter the name of the organization that holds the resources allocated by RIPE NCC. You can enter up to 256 characters. A list of words separated by white space. A word can be made up of letters, digits, the character underscore "_", and the character hyphen "-". The first character of a word must be a letter or digit and the last character of a word must be a letter, digit or a period. For example, you can enter PRNG-TEST.

**RIR Organizational Attributes**

This table lists all predefined RIR attributes associated with the RIR organization. Click the Value field of an attribute in the table to enter a value. The Required field indicates whether a value for the corresponding attribute is required.

You can add custom attributes by clicking the Add icon and select an attribute from the drop-down list. You can also delete an RIR attribute by selecting its check box and clicking the Delete icon.

For information about the attributes and how to enter their values, see RIR Organizational Attributes.

**Note:** You cannot leave an optional RIR attribute value empty. If you do not have a value for an RIR attribute, you must delete it from the table. You can enter up to 256 characters for all RIR attributes.

3. Save the configuration. Note that you cannot schedule the creation, modification, or deletion of an RIR organization.

**Modifying RIR Organizations**

To modify an RIR organization:

1. From the Administration tab, select the RIR tab -> rir_organization check box, and click the Edit icon.
2. In the Organization editor, modify the organization information, as described in Adding RIR Organizations. You can also reorder the list of RIR organizational attributes using the up and down arrows.
3. Save the configuration.

**Deleting RIR Organizations**

You can delete an RIR organization that does not have any networks assigned to it. When you delete an RIR organization, the appliance moves it to the Recycle Bin, if enabled. You can later restore the network if needed. For information about the Recycle Bin, see Using the Recycle Bin.

To remove an RIR organization:

1. From the Administration tab, select the RIR tab -> rir_organization check box, and then click the Delete icon.
2. In the Delete Confirmation (RIR Organization) dialog box, click Yes.

**Adding and Assigning RIR Networks**

Before you can assign network addresses within an RIR allocated address block to an organization, you must first add the allocated address block to NIOS. Infoblox supports IPv4 and IPv6 network containers and networks. You can also create network templates that are specific for RIR networks. For information about creating network templates, see About IPv4 Network Templates and About IPv6 Network Templates.

Note that when you add network containers or networks to NIOS, the appliance does not validate whether the corresponding networks actually exist in the RIPE database. Even though you can create the networks in NIOS, the submission of updates for the network may fail. For example, if you create a child network and the parent network is not registered in RIPE, the registration update will fail.

In addition, each network can only be associated with an RIR in one network view. If you have a network address block registered with RIPE in a
specific network view, you must not register the same address block in a different network view. When you enable the support for updates of RIR registrations, Grid Manager displays the appropriate data fields that you can use to add or modify RIR related networks. You can do the following to add IPv4 and IPv6 networks:

- Add RIR allocated IPv4 networks to NIOS, or assign addresses to specific organizations. For information see Adding IPv4 Networks.
- Add RIR allocated IPv6 networks to NIOS, or assign addresses to specific organizations. For information, see Adding IPv6 Networks.
- Add IPv4 network templates that are specific to RIR address allocation. For information, see About IPv4 Network Templates.
- Add IPv6 network templates that are specific to RIR address allocation. For information, see About IPv6 Network Templates.

You can also do the following to modify specific data about the RIR networks:

- Modify RIR allocated or assigned IPv4 networks. For information see Modifying IPv4 Networks.
- Modify RIR allocated or assigned IPv6 networks. For information see Modifying IPv6 Networks.
- Modify IPv4 network templates that are specific to RIR address allocation. For information, see Modifying IPv4 Network Templates.
- Modify IPv6 network templates that are specific to RIR address allocation. For information, see Modifying IPv6 Network Templates.

You can preview the information before the appliance submits updates to the RIPE database. To preview registration updates, click Preview RIR Submissions in the Add IPv4 Network or Add IPv6 Network wizards. For more information, see Previewing Registration Updates.

Note: You can also add RIR networks through Task Dashboard. For information, see The Tasks Dashboard.

After you create an RIR network container or network, you can perform the following:

- Split a network that has an organization ID. A child network that is created does not contain an organization ID by default. You must assign an organization ID to the child network after splitting it. For information about splitting an RIR network, see Splitting IPv4 Networks into Subnets and Splitting IPv6 Networks into Subnets.
- Resize an IPv4 RIR network that contains an organization ID and has been registered with RIPE. For more information, see Resizing IPv4 Networks.

Viewing RIR networks

You can view a list of IPv4 and IPv6 RIR networks in the Data Management tab -> IPAM tab or the Data Management tab -> DHCP tab -> Networks tab -> Networks section. For more information, see IPAM Home and Viewing Networks.

Modifying RIR Network Data

You can modify certain RIR network information in the RIR Registration tab of the IPv4 and IPv6 Network editors. To modify RIR network information, complete the following:

1. From the Data Management tab, select the IPAM tab -> network check box, and then click the Edit icon.
   or
   From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network check box, and then click the Edit icon.
2. In the IPv4 or IPv6 Network Container or Network editor, click the RIR Registration tab, and then complete the following to modify RIR related data for the IPv4 or IPv6 network container or network:
   - Internet Registry: Displays the RIR that allocates RIR address blocks. The default is RIPE. You cannot change this.
   - Organization ID: Displays the organization ID with which this network is associated. You cannot change this.
   - Registration Status: Displays the current registration status. This can be Registered or Not Registered. Registered indicates that the network has a corresponding entry in the RIPE database. Note that when you select API as the communication method, the registration status will be updated automatically after the registration update is completed. However, when you select Email as the communication method, the registration status will not be automatically updated. You can modify this by selecting the appropriate status from the drop-down list.
   - Status of last update: Displays the registration status, communication method, timestamp of the last registration update. The status can be Pending, Sent, Succeeded, or Failed. The displayed timestamp reflects the timestamp used on the Grid Master. Each time you send a registration update to create, modify, or delete a network container or network, the updated status and timestamp will be displayed here. If you have selected not to send the registration update, the previous status and timestamp are retained.
   - Registration Action: From the drop-down list, select what you want to do with the RIR network updates. If you are creating a top-level network block that has already been assigned to the organization, select None. If you are creating a child network within the allocated address block, you can select one of the following:
     - None: The appliance does not submit the updates.
     - Create: The appliance creates the network container or network for the specified organization.
     - Modify: Modifies data for this network container or network.
     - Delete: Deletes the RIR network from the organization. When you select this, you must enter a reason for deleting this entry in the Delete Reason field.
   - Do not update registrations: By default, the appliance sends updates to RIPE if you specify Create, Modify, or Delete as the registration action. Select this if you do not want the appliance to submit updates to the RIPE database.
   - RIR Network Attributes: Modify the value of RIR network attributes by clicking the Value field of an attribute and entering a new value.
You can add a new RIR network attribute by clicking the Add icon and selecting an attribute from the drop-down list. You can also select any optional attributes and click the Delete icon to delete them. For information about RIR network attributes, see RIR Network Attributes. You can enter up to 256 characters for all RIR network attributes, unless otherwise noted.

**Preview RIR Submissions**: Click this to view the updates before the appliance submits them to the RIPE database. This button is enabled only when the registration action is Create, Modify, or Delete, and the Do not update registrations check box is not selected. For more information, see Previewing Registration Updates.

To schedule this task, click the Schedule icon at the top of the wizard. In the Schedule Change panel, click Later, and then specify a date, time, and time zone.

3. Save the configuration.

### Deleting RIR Networks

When you delete an RIR network or network container, the appliance moves it to the Recycle Bin, if enabled. You must enter the reason for deleting the RIR network or network container and indicate whether you want to send the deletion update to RIPE. You can delete multiple networks at the same time.

To delete an RIR network or network container:

1. From the Data Management tab, select the IPAM tab -> network check box, and then click the Delete icon. You can choose to delete the network immediately or schedule its deletion.
2. In the Delete Confirmation (IPv4 or IPv6 Network) or Schedule Deletion dialog box, complete the following:
   - **Justification**: Enter the reason for deleting this network.
   - **Do not update registrations**: Select this check box if you do not want the appliance to submit updates to RIPE.
3. Optionally, you can click Preview RIR Submissions to view the RIR network information before deleting the network. Grid Manager displays the preview data in a separate browser window. For information, see Previewing Registration Updates.
4. Click Yes. If you are scheduling a deletion, enter the data and time for execution, and then click Schedule Deletion.

### Managing RIR Attributes

Before you can successfully submit RIR data updates, you must ensure that all RIR required attributes contain valid values that can be mapped to data in the RIPE database. The appliance does not validate data with the RIPE database before you submit your updates. The appliance also does not synchronize data from the database.

**Note**: RIPE does not support UTF-8 data in the Description and Remarks fields. After an upgrade, the NIOS appliance keeps the UTF-8 data in these fields. However, if you want to modify these fields after the upgrade, you must remove the UTF-8 data before you can save the changes.

When you enter a value for the following RIR attributes that cannot be mapped to a valid reference in the RIPE database, updates to the RIR database will fail. However, these values will still be displayed in the IPv4 or IPv6 network or network container panels of Grid Manager.

- RIPE Routes Maintainer
- RIPE Lower Level Maintainer
- RIPE Reverse Domain Maintainer
- RIPE Admin Contact
- RIPE Technical Contact
- RIPE Computer Security Incident Response Team

You can add multiple values for certain RIR attributes. When you add multiple values of the same attribute, the appliance groups the values in the order they are listed in the attribute table. You can also reorder the RIR attributes using the up and down arrows in the attribute tables.

### RIR Organizational Attributes

The following table lists RIR organizational attributes, the format you must use to enter values, and whether they are required or optional.

<table>
<thead>
<tr>
<th>Organizational Attribute</th>
<th>Corresponding RIPE Attribute</th>
<th>Description and Format</th>
<th>Required/ Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIPE Description</td>
<td>descr</td>
<td>Enter a short description about the organization.</td>
<td>Optional</td>
</tr>
<tr>
<td>RIPE Country</td>
<td>country</td>
<td>From the drop-down menu, select the country name, followed by the two-letter ISO 3166 country code, of the country or area within the RIPE NCC service region or through Local Internet Registries.</td>
<td>Required</td>
</tr>
<tr>
<td>Field</td>
<td>Type</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>RIPE Admin Contact</td>
<td>admin-c</td>
<td>Enter the name of the on-site admin contact for the organization. Enter the name in this format: Start with two to four optional characters, followed by up to six optional digits, and then follow by a source specification. The first digit cannot be &quot;0&quot;. The source specification starts with &quot;.&quot; followed by the source name that contains up to nine characters in length.</td>
<td>Required</td>
</tr>
<tr>
<td>RIPE Technical Contact</td>
<td>tech-c</td>
<td>Enter the name of the technical contact for the organization. Enter the name in this format: Start with two to four optional characters, followed by up to six optional digits, and then follow by a source specification. The first digit cannot be &quot;0&quot;. The source specification starts with &quot;.&quot; followed by the source name that contains up to nine characters in length.</td>
<td>Required</td>
</tr>
<tr>
<td>RIPE Remarks</td>
<td>remarks</td>
<td>Enter remarks about the organization.</td>
<td>Optional</td>
</tr>
<tr>
<td>RIPE Notify</td>
<td>notify</td>
<td>Enter the email address to which notifications of changes to the organization will be sent.</td>
<td>Optional</td>
</tr>
<tr>
<td>RIPE Registry Source</td>
<td>source</td>
<td>From the drop-down list, select the registry at which the organization is registered. The default is RIPE. Select RIPE for the RIPE database, which is the authoritative database. Select TEST for the RIPE TEST database that operates in the same way as the RIPE database but contains only test data. Note that test data is cleaned out at the start of each month and a predetermined set of basic objects is re-inserted. You can use the RIPE TEST database to learn how to update the database and try out special scenarios. The RIPE TEST database has fewer restrictions which allows you to create encompassing or parent objects you may need for testing.</td>
<td>Optional</td>
</tr>
</tbody>
</table>
| RIPE Organization Type | org-type | From the drop-down list, select one of the following organization type:  
- **IANA** for Internet Assigned Numbers Authority  
- **RIR** for Regional Internet Registry  
- **NIR** for National Internet Registry  
- **LIR** for Local Internet Registry  
- **WHITEPAGES** for special industry people  
- **DIRECT_ASSIGNMENT** for direct contract with RIPE NCC  
- **OTHER** for all other organizations  

**Note:** Only the RIPE database admin can set the organization type, and there are no NIRs in the RIPE NCC service region. | Optional |
<p>| RIPE Address           | address | Enter the organization address.                                                                                                                                                                          | Optional |</p>
<table>
<thead>
<tr>
<th>Network Attributes</th>
<th>Corresponding RIPE Attribute</th>
<th>Descriptions and Formats</th>
<th>Required/Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIPE Phone Number</td>
<td>phone</td>
<td>Enter the organization phone number in numeric format starting with the + character, followed by the country code, area code, and the phone number. For example, you can enter +18089991000. You can also use one of the following formats:</td>
<td>Optional</td>
</tr>
<tr>
<td>RIPE Fax Number</td>
<td>fax-no</td>
<td>Enter the organization fax number in numeric format starting with the + character, followed by the country code, area code, and the fax number. For example, you can enter +16052529000. You can also use one of the following formats:</td>
<td>Optional</td>
</tr>
<tr>
<td>RIPE Email</td>
<td>email</td>
<td>Enter the organization email address.</td>
<td>Required</td>
</tr>
<tr>
<td>RIPE Abuse Mailbox</td>
<td>abuse-mailbox</td>
<td>Enter the email address to which abuse complaints are sent.</td>
<td>Optional</td>
</tr>
<tr>
<td>RIPE Reference Notify</td>
<td>ref-nfy</td>
<td>Enter the email address to which notifications are sent when a reference to the organization object is added or removed.</td>
<td>Optional</td>
</tr>
</tbody>
</table>

**RIR Network Attributes**

When you create or edit an RIR associated network, ensure that you enter valid values for the RIR network attributes. The following table lists RIR network attributes, the format you must use to enter values, and whether they are required or optional:

<table>
<thead>
<tr>
<th>Network Attributes</th>
<th>Corresponding RIPE Attribute</th>
<th>Descriptions and Formats</th>
<th>Required/Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIPE Admin Contact</td>
<td>admin-c</td>
<td>The name of the on-site admin contact for the network address. This attribute is populated from the organizational attribute. You can modify the value in this format: Start with two to four optional characters, followed by up to six optional digits, and then follow by a source specification. The first digit cannot be &quot;0&quot;. The source specification starts with &quot;.&quot; followed by the source name that contains up to nine characters in length.</td>
<td>Required</td>
</tr>
<tr>
<td>RIPE Computer Security Incident Response Team</td>
<td>mnt-irt</td>
<td>The name of the Computer Security Incident Response Team (CSIRT) that handles security incidents for the network address. You can enter the value in this format: Use letters, digits, the character underscore &quot;.&quot;, and the character hyphen &quot;-&quot;. The value must start with &quot;irt-&quot;, and the last character of a name must be a letter or a digit. You must enter a minimum of five characters.</td>
<td>Optional</td>
</tr>
<tr>
<td>RIPE Country</td>
<td>country</td>
<td>The two-letter ISO 3166 country code of the country within the RIPE NCC service region or through Local Internet Registries. This attribute is populated from the organizational attribute. You can select a different country code from the drop-down list.</td>
<td>Required</td>
</tr>
<tr>
<td>RIPE Description</td>
<td>descr</td>
<td>Enter a short description about the network.</td>
<td>Required</td>
</tr>
<tr>
<td>RIR IPv4 Status</td>
<td>status</td>
<td>The status of the IPv4 network address. From the drop-down list, select one of the following status:</td>
<td>Required</td>
</tr>
<tr>
<td>----------------</td>
<td>--------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ALLOCATED PA</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ALLOCATED PI</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ALLOCATED UNSPECIFIED</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LIR-PARTITIONED PA</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LIR-PARTITIONED PI</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SUB-ALLOCATED PA</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASSIGNED PA</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASSIGNED PI</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASSIGNED ANYCAST</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EARLY-REGISTRATION</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOT-SET</td>
<td>-----------</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RIR IPv6 Status</th>
<th>status</th>
<th>The status of the IPv6 network address. From the drop-down list, select one of the following:</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ALLOCATED-BY-RIR</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ALLOCATED-BY-LIR</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASSIGNED</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASSIGNED ANYCAST</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASSIGNED PI</td>
<td>-----------</td>
</tr>
</tbody>
</table>

| RIR Lower Level Maintainer | mnt-lower | Enter the name of the registered maintainer for hierarchical authorization purposes. This can protect the creation of networks directly (one level) below the hierarchy of a network container or another network. The authentication method of the maintainer will be used upon creation of any network directly below the network that contains the "mnt-lower:" attribute. Enter the maintainer name in this format: Use letters, digits, the character underscore "\_", and the character hyphen "\-". The first character must be a letter, and the last character must be a letter or a digit. You cannot use the following words (they are reserved by RPSL): any, as-any, rs-any, peer, as, and, or, not, atomic, from, to, at, action, accept, announce, except, refine, networks, into, inbound, outbound. Also note the following: Names starting with certain prefixes are reserved for certain object types. Names starting with "as-" are reserved for as set names. Names starting with "rs-" are reserved for route set names. Names starting with "irt-" are reserved for irt names. Names starting with "prng-" are reserved for peering set names. Names starting with "mnt-lower:" are reserved for parent objects you may need for testing. | Optional |

| RIR Network Name | netname | The name of the IP address range. You can enter up to 80 characters. Enter the network name in this format: Use letters, digits, the character underscore "\_", and the character hyphen "\-". The first character must be a letter, and the last character must be a letter or a digit. | Required |

| RIR Notify | notify | Enter the email address to which notifications of changes to the object must be sent. | Optional |

| RIR Registry Source | source | From the drop-down list, select the registry at which the organization is registered. The default is RIPE. Select RIPE for the RIPE database, which is the authoritative database. Select TEST for the RIPE TEST database that operates in the same way as the RIPE database but contains only test data. Note that test data is cleaned out at the start of each month and a predetermined set of basic objects is re-inserted. You can use the RIPE TEST database to learn how to update the database and try out special scenarios. The RIPE TEST database has fewer restrictions which allows you to create encompassing or parent objects you may need for testing. | Required |

| RIR Remarks | remarks | Enter remarks about the network. | Optional |

| RIR Reverse Domain Maintainer | mnt-domains | Enter the name of a registered maintainer used for reverse domain authorization. This can protect domain objects. The authentication method of this maintainer will be used for any encompassing reverse domain object. Enter the maintainer name in this format: You can use letters, digits, the character underscore "\_", and the character hyphen "\-". The first character must be a letter, and the last character must be a letter or a digit. You cannot use the following words (they are reserved by RPSL): any, as-any, rs-any, peer, as, and, or, not, atomic, from, to, at, action, accept, announce, except, refine, networks, into, inbound, outbound. Also note the following: Names starting with certain prefixes are reserved for certain object types. Names starting with "as-" are reserved for as set names. Names starting with "rs-" are reserved for route set names. Names starting with "irt-" are reserved for irt names. Names starting with "prng-" are reserved for peering set names. Names starting with "mnt-lower:" are reserved for parent objects you may need for testing. | Optional |

| RIR Routes Maintainer | mnt-routes | This attribute references a maintainer that is used in determining authorization for the creation of route objects. Enter the name in this format: Start with the reference to the maintainer, followed by an optional list of prefix ranges inside of curly brackets or the keyword "ANY". The default, when no additional set items are specified, is "ANY". For more information, refer to RFC-2822. Example: &lt;mnt-name&gt; { [ list of &lt;address-prefix-range&gt; ] | ANY | }. | Optional |

| RIR Technical Contact | tech-c | The name of the technical contact for the network. Enter the name in this format: Start with two to four optional characters, followed by up to six optional digits, and then follow by a source specification. The first digit cannot be "0". The source specification starts with "\" followed by the source name that contains up to nine characters in length. | Required |

---

**Monitoring RIR Data**

You can view RIR organizations and networks you added to NIOS through Grid Manager. The appliances sends SNMP traps and email notifications about registration updates. It also logs RIR events in the Infoblox syslog. Note that sometimes due to network timeout from RIPE, your registration updates may fail. You can do the following to monitor RIR data:

- View RIR update events in the syslog, as described in Viewing the Syslog.
- View RIR organizations, as described in Viewing RIR Organizations.
- View RIR IPv4 and IPv6 network containers and networks, as described in IPAM Home and Viewing Networks.
- Preview RIR updates before submitting them to RIPE, as described in Previewing Registration Updates.

**Viewing RIR Organizations**

You can view the list of RIR organizations that have received address allocation and the ones you have added associated networks. To view RIR organizations:

1. From the Administration tab, select the RIR tab.
2. Grid Manager displays the following information for each RIR organization:
   - **Organization ID**: The RIR organization ID.
   - **RIR**: The RIR that allocates the address block to the organization.
   - **Maintainer**: The name of the maintainer for the organization.

You can also select Organization Name and RIR organizational attributes for display.

You can do the following in this tab:

- Modify some of the data in the table. Double click a row, and either modify the data in the field or select an item from a drop-down list.
- Sort the data in ascending or descending order by column.
- Select an organization and click the Edit icon to modify data, or click the Delete icon to delete it.
- Click the Permissions icon to configure permissions for the admin account.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information about quick filters, see Using Quick Filters.
- Print and export the data in this tab.

**Previewing Registration Updates**

Before the appliance submits RIR updates to RIPE, you can preview the data in Grid Manager. The appliance uses the email template when displaying preview data in a separate browser window.

Preview data includes the subject line for the email, followed by the inetnum or inet6num template for the network and other associated data, such as network name, organization name, and others. When there are multiple operations involved, such as deleting multiple networks, the preview data includes a separate subject line for each operation.

You can preview registration updates when you create a new RIR network. In the Add Networks wizard, click Preview RIR Submissions in the wizard. For information about how to create or assign RIR networks, see Adding and Assigning RIR Networks.

Following is a sample preview for a network creation request:

```
Subject: CREATE inetnum 100.200.0.0 - 100.200.255.255
KEYWORDS: NEW inetnum: 100.200.0.0 - 100.200.255.255
netname: corpxyz_network
descr: RIR network for corpxyz. status: ASSIGNED PA
org: ORG-MC1-TEST
country: US source: TEST
changed: jdoe@corpxyz.com 20120809 notify: jdoe@corpxyz.com
admin-c: NP1-TEST tech-c: NP1-TEST mnt-by: JohnDoe password: ***
```

Following is a sample preview for a network modification request:

```
Subject: MODIFY inetnum 100.200.0.0 - 100.200.255.255
KEYWORDS: inetnum: 100.200.0.0 - 100.200.255.255
netname: corpxyz_network
descr: RIR network for corpxyz. status: ASSIGNED PA
org: ORG-MC1-TEST
country: US source: TEST
changed: jdoe@corpxyz.com 20120809 notify: jdoe@corpxyz.com
admin-c: NP1-TEST tech-c: NP1-TEST mnt-by: JohnDoe password: ***
```

Following is a sample preview for deleting multiple networks:

```
Subject: DELETE inetnum 100.200.0.0 - 100.200.255.255
KEYWORDS: inetnum: 100.200.0.0 - 100.200.255.255
netname: corpxyz_network
descr: RIR network for corpxyz. status: ASSIGNED PA
org: ORG-MC1-TEST
country: US source: TEST
changed: jdoe@corpxyz.com 20120809 notify: jdoe@corpxyz.com
admin-c: NP1-TEST tech-c: NP1-TEST mnt-by: JohnDoe password: ***
delete: Removed network.
```

```
Subject: DELETE inetnum 100.300.0.0 - 100.300.255.255
KEYWORDS: inetnum: 100.300.0.0 - 100.300.255.255
netname: corp200_network
```
Part 3 IP Address Management

IPAM (IP Address Management) is the allocation, administration, reporting, and tracking of IP addresses, network devices, and their associated data. This section provides information about IPAM and how to use the Infoblox tools to perform IPAM tasks and manage your entire IP network. It includes the following chapters:

- Chapter 13, IP Address Management
- Chapter 14, IP Discovery and vDiscovery
- Chapter 15, Infoblox Network Insight

Chapter 13 IP Address Management

This chapter describes how to manage your networks and IP addresses through the Infoblox IPAM (IP Address Management) implementation. It contains the following sections:

- About IP Address Management
- About Host Records
  - Assigning Multiple IP Addresses to a Host
  - Adding Host Records
  - Copying and Modifying Host Records
- About Network Containers
  - Adding IPv4 and IPv6 Network Containers and Networks
  - Modifying IPv4 and IPv6 Network Containers and Networks
  - Deleting Network Containers
- Managing IPv4 Networks
  - IPv4 Network Map
  - IPAM Home
  - Resizing IPv4 Networks
  - Splitting IPv4 Networks into Subnets
  - Joining IPv4 Networks
  - Discovering Networks (Under Network Insight only)
- Viewing and Managing IPv4 Addresses
  - IP Map
  - IPv4 Address List
  - Managing IPv4 Addresses
  - Managing IPv4 Addresses
- Managing IPv6 Networks
  - IPv6 Network Map
  - IPv6 Network List
  - Splitting IPv6 Networks into Subnets
  - Joining IPv6 Networks
- Viewing IPv6 Data
- Viewing Identity Mapping Information
  - Viewing Active Network Users
  - Viewing Network Users Login History
- Managing IPv4 and IPv6 Addresses
  - Converting Objects Associated with IP Addresses
  - Reclaiming Objects Associated with IPv4 and IPv6 Addresses
  - Pinging IPv6 Addresses
  - Clearing Active DHCP Leases
- Configuring Thresholds for IPAM Utilization
- About Network Insight
- Viewing Identity Mapping Information
  - Viewing Active Network Users
  - Viewing Network Users Login History
  - Configuring Active User Timeout Session

About IP Address Management

IPAM is the allocation, administration, reporting, and tracking of public and private IP spaces, network devices, and their associated data. It comprises the deployment of DNS and DHCP services and the monitoring of network devices and performance to ensure data integrity and security of your networks.

The Infoblox IPAM implementation is a feature-rich and easy-to-use solution that encompasses support for IPv4, IPv6, network discovery, and...
Infoblox IPAM provides tools that integrate the allocation, administration, reporting, and tracking of your entire network space. Figure 13.1 highlights the Infoblox IPAM implementation.

**Figure 13.1 Infoblox IPAM Features**

<table>
<thead>
<tr>
<th>Allocation</th>
<th>Administration</th>
<th>Reporting</th>
<th>Tracking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure networks and allocate IP addresses to network devices. Resize, join, or split networks. Use Infoblox host records to centralize the management of DNS and DHCP data.</td>
<td>Use network maps and IP maps to view and administer your entire network space, and manage the IP addresses of your network devices.</td>
<td>The Dashboard provides widgets that monitor IPAM and network statistics. The syslog and audit log provide detailed information about system and admin activities. The reporting solution automates the collection, analysis, and presentation of core network device data. Use network discovery to track your network devices and monitor network performance. Configure how you want the Infoblox appliance to populate the discovered data. Use DHCP fingerprint detection to track network devices, block those that are not allowed, and plan for future growth.</td>
<td></td>
</tr>
</tbody>
</table>

You can perform the following IPAM tasks to effectively manage and control your network:

- Create host records. Host records integrate the DNS records and DHCP data of a network device. You can use a host record to manage a network device from one central point. For more information, see *About Host Records*.
- Create IPv4 and IPv6 networks. For information, see *About Network Containers*.
- Discover devices in IPv4 and IPv6 networks and other Objects created in IPAM. For more information, see *Adding IPv4 and IPv6 Network Containers and Networks*, *Adding Host Records* and other sections throughout this chapter. View your IPv4 network and address utilization in a graphical mode. For information, see *IPv4 Network Map* and *IP Map*.
- When necessary, resize, join, or split networks. For information, see *Resizing IPv4 Networks*, *Splitting IPv4 Networks into Subnets*, *Joining IPv4 Networks*, *Managing IPv4 and IPv6 Addresses*, *Add and manage DNS resource records associated with IP addresses*. For information, see *DNS Resource Records*.
- Monitor your core service network data using the Dashboard, audit log, syslog, and reports. For information, see *Part 7 Monitoring and Reporting*.
- Discover and track network devices. For information, see *IP Discovery and vDiscovery* and *DHCP Fingerprint Detection*.

**About Host Records**

Host records provide a unique approach to the management of DNS, DHCP, and IPAM data. By using host records, you can manage multiple DNS records and DHCP and IPAM data collectively, as one object on the appliance.

When you create a host record, you are specifying the name-to-address and address-to-name mappings for the IP address that you assign to the host. The Infoblox DNS server then uses this data to respond to DNS queries for the host. When the server receives a name-to-address query, it responds with an A record for an IPv4 host or an AAAA record for an IPv6 host that contains the data from the host record. Likewise, when it receives an address-to-name query for the host, the appliance responds with a PTR record that contains data from the host record.

**Note:** The appliance cannot respond if there is no PTR record and a PTR record is not created if there is no corresponding reverse-mapping zone.

Additionally, if you specify an alias in the host record, the appliance uses this data as a CNAME record to respond to queries with the alias. It maps the alias to the canonical name and sends back a response with the canonical name and IP address of the host. Thus, a single host record is equivalent to creating A, PTR, and CNAME resource records for an IPv4 address and AAAA and PTR records for an IPv6 address. The appliance supports IDNs for a host record. You can specify alias and domain names in the native character set. For information about IDN support, see *Support for Internationalized Domain Names*.

Hosts also support prefix delegation for IPv6. For example, you can specify an IPv6 prefix in the host record of a router. The router then advertises this prefix on one of its interfaces, so hosts that connect to the interface can generate their IP addresses, using the stateless autoconfiguration mechanism defined in *RFC 2462, IPv6 Stateless Autoconfiguration*.

In addition, if the Infoblox DHCP server manages the IP address assigned to the host, the server uses it as a fixed address record as well. The DHCP server assigns the IP address to the host when it receives a DHCP request with the matching MAC address or DUID. Its response includes configuration information, and any DHCP options defined for the host or inherited from the network to which the fixed address belongs. You can
also assign multiple IPv4 and IPv6 addresses to a host, as described in Assigning Multiple IP Addresses to a Host. You can copy an existing host record and turn it into a new one. When you copy a host record, other than the new host name and IP address, all DHCP and IPAM configuration including the MAC address and extensible attributes apply to the new record. You can also modify information, except for the host name and IP address, of an existing host record. For information about how to copy or modify a host record, see Copying and Modifying Host Records. Note that you can also modify an IPv4 host record and turn it into a IPv4 reservation. For information, see Configuring IPv4 Reservations.

You can execute immediate discovery on a host record. This simple setting enables you to determine the precise type of device that is associated with the host, along with its IP addresses, its name and other information.

You can define extensible attributes for a host record to further describe the device. You can include information such as its location and owner for IP address management purposes. For information about extensible attributes, see About Extensible Attributes.

Figure 13.2 Using the Host Record for DHCP and DNS

Figure 13.2 Using the Host Record for DHCP and DNS

Note that if the zone of the host record is associated with networks, the IP addresses must belong to the associated networks. For example, if the host record is in the corp.xyz.com zone, which is associated with 10.1.0.0/16 network, then the IP addresses of the host record must belong to the 10.1.0.0/16 network. For information about associating zones and networks, see Associating Networks with Zones.

Assigning Multiple IP Addresses to a Host

You can assign multiple IPv4 and IPv6 addresses to a host depending on the function of the device. For example, you can create a host record for a router that supports three network interfaces in two different networks, and assign IP addresses to each interface, as illustrated in Figure 13.3. When the DNS server responds to DNS queries for the host, it includes an A or AAAA record for each IP address.

In addition, if the IP addresses belong to different networks, they can have different DHCP configurations and options. As shown in Figure 13.3, the configuration information and DHCP options of the interface with the IPv6 address 2001:db8:1::2 may be different from the other two interfaces, 10.31.209.5 and 10.31.209.7, because it is in a different network.

Figure 13.3 Assigning Multiple IP Addresses to one Host Record
Adding Host Records

You can add host records from the Toolbar of the IPAM, DHCP and DNS tabs of the Data Management tab and from the Tasks Dashboard. For information about the Tasks Dashboard, see The Tasks Dashboard.

When you create a host record, you must specify its zone and at least one IP address. If the zone of the host record is associated with one or more networks, the IP addresses must belong to one of the associated networks. If a zone of a host record contains IDNs, the appliance displays the zone name in the native character set.

For Cloud Network Automation, you can create host records within a delegated network view only when you enable DNS for the host record.

To add a host from the Data Management tab:

1. From the IPAM, DHCP or DNS tab of the Data Management tab, expand the Toolbar.
2. Click Add and select the option to add a host from the drop-down menu.
3. In the first page of the Add Host wizard, do the following:

   - **Name:** If Grid Manager displays a zone name, enter the host name here. The displayed zone name can either be the last selected zone or the zone from which you are adding the host. If no zone name appears or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter a unique name for the host. The name you enter is prefixed to the DNS zone name that is displayed, and the complete name becomes the FQDN (fully qualified domain name) of the host. For example, if the zone name displayed is corpxyz.com and you enter admin, then the FQDN is admin.corpxyz.com.
   - **Enable in DNS:** This is selected by default. It enables DNS service for the host. If you clear this check box, DNS does not serve this host and you cannot assign it to a zone.
   - **Protected:** This is selected by default. To mark the record as protected in order to restrict DDNS updates to this record, select the Protected check box. This applies to both static and dynamic records.

   **Note:** If you select to protect the record, ensure that you also select the Prevent dynamic updates to RRsets containing protected records check box in the advanced updates properties of the Grid, view, zone, or Standalone appliance.

Alternatively, you can protect records by selecting them, individually or in bulk, in the Resource Records Viewer and clicking Protect Records -> Enable Protection in the Toolbar.

- **DNS View:** Displays the DNS view for the host record. This appears only when you enable the host record in DNS.
- **Host Name Policy:** Displays the host name policy of the selected zone. This appears only when you enable the host record in DNS.
- **RRset Order:** Select one of the following RRset orders that the appliance uses to return A and AAAA records of the host. This check box appears only when you have enabled the configuration of RRset order for the Grid and there are multiple IP addresses in this host record. For information about how to enable this feature, see Enabling the Configuration of RRset Orders.
  - **Cyclic:** The records are returned in a round robin pattern. This is the default.
  - **Fixed:** The records are returned in the order you specify in this host record. When you select this check box, the appliance displays up and down arrows next to the IPv4 and IPv6 address tables. You can use these arrows to reorder the address list. The appliance returns the A and AAAA records of this host based on the order you define in the address tables.
  - **Random:** The records are returned in a random order.

   Note that when you specify Fixed as the RRset order, the appliance places the resource records as follows:
   - A and AAAA records of the host in the fixed order you specify in the address tables. Note that the order of the returned A and AAAA records are independent of each other.
   - Other A and AAAA records in an undefined order.
   - Other record types in the default cyclic order.

   For more information about RRset order, see Enabling the Configuration of RRset Orders.

- In the IPv4 Addresses and IPv6 Addresses sections, specify the IP addresses of the host record. Click the Add icon do one of the following:
  - **Select Next Available IP Address** to retrieve the next available IP address in a network. Infoblox recommends this option to ensure that you assign an IP address from the appropriate network.
    - If the host record is in a zone that has one associated network, Grid Manager retrieves the next available IP address in that network.
    - If the host record is in a zone that has multiple associated networks, the Network Selector dialog box lists the associated networks. If the zone has no network associations, the Network Selector dialog box lists the available networks. When you select a network, Grid Manager retrieves the next available IP address in that network.
    - If you want to enter a link-local IPv6 address, you must enter an IPv4 address and the host MAC address first, and then click the Add (+) icon again to enter the link-local IPv6 address. When you select the link-local IPv6 address, the MAC address is automatically filled in. For information, see Understanding DNS for IPv6.
    - Optionally, you can delete an IP address from the host by selecting an IP address in the table and clicking the Delete icon.
  - or
    - **Select Add Address** to enter an IPv4 or IPv6 address. You can also enter an IPv6 prefix. Note that when you use this option, you could specify an IP address from a network that has not yet been defined. To avoid this, use the Next Available IP Address option instead.
    - **MAC Address:** For an IPv4 address, enter the MAC address of the network device associated with this host IP address. Note that you must enter a MAC address if DHCP is enabled for the host IP address.
    - or
    - **DUID:** For an IPv6 address, enter the DHCP Unique Identifier (DUID) of the network device associated with this host IP address. Note that you must enter a DUID if DHCP is enabled for an IPv6 host address.
• **DHCP**: Select this to enable the DHCP services to manage the host IP address. If you do not select this option, the host IP address is not managed by the DHCP server.

• **Comment**: Optionally, enter additional information about the host record.

• **Disable**: Select this option to temporarily disable the host record. For example, you might want to disable a host when you need to update the network device.

The **Cloud** section appears when the Cloud Network Automation license is installed on the Grid Master. For information, see Deploying Cloud Network Automation. This section displays the following information:

• **Cloud Usage**: This field indicates whether this object is associated with any specific cloud extensible attributes or within a scope of delegation. It can be one of the following:
  - **Cloud from adapter**: Indicates that this object has been created by a cloud adapter and it may or may not be within a scope of delegation at the moment.
  - **Cloud from delegation**: Indicates that this object is within the scope of delegation or the object itself defines a scope of authority delegation, and it is not created by a cloud adapter.
  - **Used by cloud**: Indicates that this network or network container is associated with the extensible attribute Is External or Is Shared and the value is set to True, which implies the network is a private or shared network managed by the CMP, and it is not Cloud from adapter or Cloud from delegation.
  - **Non-cloud**: The object is a regular NIOS object and is not within the scope of any authority delegation nor is it associated with any of these extensible attributes: Cloud API Owned, Is External or Is Shared. NIOS admin users can modify this object based on their permissions.

• **Owned By**: A cloud object can be owned by the Grid Master or the cloud adapter. When the object is created by the Grid Master, this shows Grid. If the object is created by the cloud adapter, this shows Adapter. Delegate authority from the Grid Master

• **Delegate To**: This field indicates whether the authority for the object you want to create has already been delegated. If so, it displays the name of the delegation.

4. **(Applies only to Network Insight)** In the current Wizard step, you can optionally define the following identification values and settings for the new object's port reservation:

   • Choose the Device Type: Router, Switch-Router, Switch, MSFT (Microsoft) Server, NetMRI, NIOS, VNIO, or ESX (VMware) Server.
   
   The values on this page are not required for defining the actual port reservation in a later wizard step.

   • Choose the Device Vendor: Cisco, Juniper, Aruba, Dell, Infoblox, or HP.

   • You can also enter a Location and a Description. These values are advisory and not required for configuration.

5. **(Applies only with Network Insight)** Click **Next** to initiate or disable discovery of the new host.

   • Choose either **Exclude from Network Discovery** or **Enable Immediate Discovery**. If you choose to Exclude, discovery will not execute on the host. If you choose **Enable Immediate Discovery**, discovery will execute on the host after you save your settings. You may also choose to disable both options.

   • By default, the new host inherits its SNMP credentials from those defined at the Grid level. Should you wish to override them for a local set of credentials, check the **Override Credentials** check box and select the **SNMPv1/SNMPv2** or **SNMPv3** option and enter the locally used credentials. For more information, see the sections Configuring SNMPv1/v2 Credentials for Polling and Configuring SNMPv3 Properties for a complete description of SNMP credentials for discovery. (You can also test SNMP credentials to ensure they work before use.)

   • For the new object, you can check the **Override CLI Credentials** check box to override the inherited set of CLI credentials taken from the Grid level. This set of credentials may be used for the device that is directly associated with the new object (in this case, a Host) in its port reservation.

   • You can also click **Test CLI Credentials** to enter and test a set of CLI login credentials against a device based on its IP address. Port control operations require CLI credentials for the involved devices. (If you are not using port control for the new object, usage of CLI credentials is optional.) Because some IPAM and DHCP objects will use port control features as part of object creation, CLI credentials are automatically leveraged as part of discovery. Ensure you have the correct sets of CLI credentials for devices in your network. For more information, see the section Configuring CLI Discovery Properties.

   • SSH is the default for CLI operations. Check the **Allow Telnet** check box if you know the device involved in the object assignment may support Telnet but may not support SSH, or if you want Telnet as an option.

6. **(Applies only with Network Insight)** Click **Next** to define switch port connectivity for the device that will be associated with the new host record. This step is optional and not required for creating the new host record. This feature set is also termed port control in Grid Manager. The device to which the new host record will be associated should already be discovered and managed from Grid Manager.

   • Begin by checking the Reserve Port check box. Note that reserving a switch port does not guarantee its availability. Optionally, you can skip connecting port configuration by clicking Next.

   • Click the **Clear** button to remove the selected device from the configuration.

   • Click the Select Device button to choose the device for which the port reservation will be associated. You should know the identity of the device to whose interface the new object will be associated before taking this step. For more information, see the section Using the Device Selector.

   • After choosing the device, choose the Interface with which the port reservation will be bound. The drop-down list shows only interfaces that are most recently found to be available by Grid Manager during the last discovery cycle. This list will not include any ports that are Administratively Up and Operationally Up or that are otherwise already assigned to other networks or objects.

   • The Wizard page also shows a list of any VLANs that are currently configured in the chosen device (The following VLANs are configured). This Wizard page allows you to assign an existing VLAN in the chosen device to the new port reservation.

   • Check the Configure Port check box to define specific port control settings for the port reservation.

   • Choose the Data VLAN and/or the Voice VLAN settings you may need for the port assignment. Depending on the selected device, you may or may not be able to apply VLAN settings.

   • Set the Admin Status to Up if you need to activate the port after assignment in the current task.

   All port control operations require CLI credentials to be entered into Grid Manager. Because some IPAM and DHCP objects will
use port control features as part of object creation, CLI credentials are automatically leveraged as part of discovery and configuration of port configurations such as Admin Up/Down status.

Ensure you have the correct sets of CLI credentials for devices in your network.

- Enter a Description for the port assignment. Infoblox recommends doing so to help other technicians to recognize the port assignment task.

7. Click Next to define extensible attributes. For information, see Using Extensible Attributes.

8. As the final step in the Add Host wizard, you define when Grid Manager creates the new object by scheduling it. As a separate task, you also schedule when the associated Port Configuration task executes.

- To create the new Host and its associated port reservation immediately, select Now. The port control event is automatically synchronized to take place at the same time as the activation of the new host.
- You can choose to have Grid Manager execute the port reservation at the same time as the host object creation. To do so, select At same time as Host.
- You can have Grid Manager execute the port reservation at a later time by selecting Later. Choose a Selected time by entering or selecting a Start Date (click the calendar icon to choose a calendar date) and a Start Time, and choose a Time Zone.

9. Choose one of the following from the Save & ... drop-down button menu:

- Click Save & Close to add the Host object and close the wizard (this is the default).
- Click Save & Edit to add the Host object and launch the editor.
- Click Save & New to add the Host object and launch the wizard again to add another Host object.

Copying and Modifying Host Records

You can create a new host record by copying an existing one. When you copy a host record, other than the new host name and IP address, all DHCP and IPAM configuration including the MAC address and extensible attributes apply to the new record. You can also modify information, except for the host name and IP address, of an existing host record.

To copy or modify an existing host record:

1. From the Data Management tab, select the IPAM, DHCP, or DNS tab.
2. In the selected tab, search for or navigate to the host record that you want to copy or modify.
3. Do one of the following:
   - To copy a host record, select the record and expand the Toolbar, and then click Add -> Host -> Copy Host. Grid Manager displays the Host Record editor.
   - To modify a host record, select the record and click the Edit icon. Grid Manager displays the Host Record editor.
4. The Host Record editor provides the following tabs from which you can modify all the fields:

   - **General**: Enter the new hostname and specify at least one IP address. Optionally, you can modify the information you entered through the wizard as described in Adding Host Records. Note that when you are modifying a DHCP enabled host address, you can apply IPv4 logic filters. To apply IPv4 logic filters, complete the following in the IPv4 Addresses section:
     - Select the IP address and click the Edit icon.
     - Click the IPv4 Filters tab in the Advanced tab and complete the following:
       - IPv4 Filters: You can keep the inherited IPv4 logic filters or override them and add a new IPv4 logic filter. For information, see Applying Filters to DHCP Objects.
   - **Device Information**: You can change advisory Device Information settings for the object's port reservation; settings are described in the section Adding Host Records.
   - **TTL**: This tab displays the default TTL settings the record inherited from the Grid or the DNS zone, if you enabled override TTL settings at the zone level. You can keep the default settings or override them. To override the inherited value, click Override to enable the configuration. Specify how long the record is cached. Select the time period in seconds, minutes, hours, days, or weeks from the drop-down list. To enable the record to inherit the Grid or zone TTL settings, click Inherit.
   - **Aliases**: Click the Add icon. Grid Manager displays a new row in the table. Enter a fully qualified domain name (a CNAME record for the host) in the Aliases column. You can delete an alias by selecting the alias check box and clicking the Delete icon.
   - **IPv4 Discovered Data**: Displays the discovered data of the IPv4 addresses, if any, of the host record. For information, see Viewing Discovered Data.
   - **Port Reservation**: Review and edit any device port reservations that may be defined for the current object, or create a new port reservation and schedule it. For a closer look, see the section Port Control Features in Network Insight, and steps 4-8 in the section Adding Host Records.
   - **IPv6 Discovered Data**: Displays the discovered data of the IPv6 addresses, if any, of the host record. For information, see Viewing Discovered Data.
   - **Extensible Attributes**: You can add and delete extensible attributes that are associated with a host record. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see About Administrative Permissions.
5. Save the configuration and click Restart if it appears at the top of the screen.

About Network Containers

Grid Manager uses network containers to group IPv4 and IPv6 networks. A network container is a parent network that contains other network containers and leaf networks. A leaf network is a network that does not contain other networks. For example, Figure 13.4 illustrates the IPv4 20.0.0.0/8 network, which is a network container with two network containers, 20.8.0.0/13 and 20.72.0.0/13. The 20.8.0.0/13 network has two leaf networks, 20.8.0.0/16 and 20.9.0.0/16. The 20.72.0.0/13 network has one leaf network, 20.72.0.0/16.

*Figure 13.4 IPv4 Network Container*
From Grid Manager, you can click the link of the network container 20.0.0.0/8 in the IP List panel and drill down to the two network containers, 20.8.0.0/13 and 20.7.0.0/13, as shown in Figure 13.5. You can click the network container links to drill down further to the leaf networks.

Figure 13.5 IP List View of Network Containers

In the IPAM tab, when you create an IPv4 or IPv6 network that belongs to a larger network, the appliance automatically creates a network container and puts the leaf network in the container. The appliance also creates network containers when you split IPv4 or IPv6 networks into smaller networks. For information, see Splitting IPv4 Networks into Subnets and Splitting IPv6 Networks into Subnets.

Adding IPv4 and IPv6 Network Containers and Networks
To add an IPv4 or IPv6 network container or network:

1. From the Data Management tab, select the IPAM tab.
2. Click the Add icon and select either IPv4 Network or IPv6 Network.
3. In the Add Network wizard, create a network as described in Adding IPv4 Networks or Adding IPv6 Networks.

Modifying IPv4 and IPv6 Network Containers and Networks
You can modify existing network settings, with the exception of the network address and subnet mask. To modify an IPv4 or IPv6 network container or network:
Managing IPv4 Networks

Deleting Network Containers

Depending on the configuration, you may or may not be able to delete or schedule the deletion of a network container and all its contents. Contents in a network container can include other network containers, leaf networks, and associated objects. For recursive deletions, only network containers and networks are considered. Objects such as hosts are not considered for recursive deletions.

Superusers can determine which group of users are allowed to delete or schedule the deletion of a network container and all its contents. For information about how to configure the recursive deletion of network containers, see Configuring Recursive Deletions of Networks and Zones.

The appliance puts all deleted objects in the Recycle Bin, if enabled. You can restore the objects if necessary. When you restore a parent object from the Recycle Bin, all its contents, if any, are re-parented to the restored parent object. For information about the Recycle Bin, see Using the Recycle Bin.

To delete a network container:

1. From the Data Management tab, select the IPAM tab -> network_container check box. You can select multiple network containers for deletion.
2. Click the Delete icon.
3. Do one of the following in the Delete Confirmation dialog box:
   - Select one of the following. Note that these options appear only if you are allowed to delete the network container and all its contents. For information about how to configure this, Configuring Recursive Deletions of Networks and Zones.
   - **Delete only the network container and re-parent the subnets**: Select this to delete only the network container and re-parent its subnets.
   - **Delete the network container and all its subnets**: Select this to delete both the network and its contents.
   - **Click Yes**.

The appliance puts the deleted network container in the Recycle Bin, if enabled. You can also schedule the deletion for a later time. Click Scheduling Deletions and in the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Deletions. For information about scheduling recursive deletions of network containers, see Scheduling Recursive Deletions of Network Containers and Zones.

Managing IPv4 Networks

In Grid Manager, you use the Net Map (network map) and List panels to manage your IPv4 network infrastructure. After you select a network container from the IPAM tab, Grid Manager displays it in the Net Map panel, by default. The Net Map panel provides a graphical view of your networks and has a number of features that simplify network management. The List panel displays the networks in table format.

You can always switch your view of a network container between the Net Map and List panels. Grid Manager keeps track of which panel you last used. For information about each panel, see IPv4 Network Map and IPAM Home.

Use the IP Map and List panels to manage the IP addresses in leaf networks. For information, see Viewing and Managing IPv4 Addresses.

After you create an IPv4 network, you can modify its properties, resize it, use the split network feature to create subnets, enable discovery to discover routers, switches, firewalls, wireless access points and other device types within it, or join it to another network to create a larger network that encompasses adjacent subnets. You can do the following from both the Net Map and List panels:

- **Resize a network**. For information, see Resizing IPv4 Networks.
- **Split a network into subnets**. For information, see Splitting IPv4 Networks into Subnets.
- **Join a network**. For information, see Joining IPv4 Networks.
- **Discover devices in the network**. For information, see Discovering Networks (Under Network Insight only).

IPv4 Network Map

After you select an IPv4 network container from the IPAM tab, Grid Manager displays it in the Net Map (network map) panel, by default. Net Map provides a high-level view of your IPv4 network address space. You can use Net Map to design and plan your network infrastructure, configure and manage individual networks, and evaluate their utilization. Its unique display of the IPv4 network address space across multiple rows is similar to a road map that starts with the first IP address in the network and ends with the last address. Net Map displays the network address space across a maximum of eight rows, depending on the size of the network. It automatically scales the map so that it displays the entire address space of a network container.

The Net Map panel presents a complete view of the network space, including the different types of networks that are in it and its unused address space. IP addresses that belong to a network are blocked off. Each color-coded block represents a network container, a leaf network, or a block of networks that are too small to be displayed individually in the map. For example, in a /8 or /16 network, networks smaller than /20 or /28 respectively and that are beside each other are represented as a multiple network block. In addition, the fill pattern of the blocks indicates their utilization. Therefore, you can quickly evaluate how many and what type of networks are in a network container, their relative sizes, utilization, and how much space you have left.

As you mouse over areas of the map, it displays IP information about the area. Net Map also has a zoom feature that allows you to enlarge or reduce your view of a particular area.

Figure 13.6 displays the network map of a 20.0.0.0/8 network, which is a network container that has network containers and leaf networks.

Figure 13.6 20.0.0.0/8 Network Map
Displaying IP Information
As shown in Figure 13.6, as you mouse over the map, Net Map displays IP information about the area. When you mouse over an unused area, Net Map displays the following information:

- The start and end IP address
- The number of IP addresses that can fit in that space
- The largest possible network
- The number of /16 and /24 networks that can fit in that space

When you mouse over a network, Net Map displays the following information:

- Network address and netmask
- Utilization of the network. For a leaf network, Net Map reports the percentage of used IP addresses, except the broadcast and network addresses. For a network container, Net Map reports the percentage of the IP address space that has been allocated to either network containers or leaf networks.
- The first and last IP address of the network
- The total number of IP addresses in the network

When you mouse over a block of multiple networks, Net Map displays the following information:

- The start and end IP address of that block of networks
- The total number of IP addresses in that block of networks
- The number of networks in that block

Zooming In and Out

Use the zoom function to enlarge and reduce your view of a selected area. You can zoom in on any area in your network. You can zoom in on an area until it displays 128 addresses per row, for a total of 1024 addresses for the map. When you reach the last possible zoom level, the Zoom In icon in the Net Map task bar and the menu item are disabled.

After you zoom in on an area, you can click the Zoom Controller icon to track where you zoomed in. The Zoom Controller lists all the areas that you zoomed in and updates its list dynamically. You can click an item on the list to view that area again. Click the Zoom Controller again to close it.

To select an area and zoom in:
1. Right-click and select **Zoom In**, or click the Zoom In icon in the Net Map task bar. The pointer changes to the zoom in selector.
2. Select a starting point and drag to the end point. The starting point can be anywhere in the map. It does not have to be at the beginning of a network.

Net Map displays a magnified view of the selected area after you release the mouse button. As you mouse over the zoomed in area, Net Map displays IP information about it.
3. You can do the following:
   - Select an area and zoom in again.
   - Add a network. If you zoom in on an area and click Add without selecting an open area first, Net Map selects the area where it can create the biggest possible network in that magnified area.
   - Select a network and perform any of the following operations:
     - Split the network.
     - Join it to another network.
     - Resize the network.
     - Edit its properties.
     - Open it to display its network or IP map.
   - Right-click and select **Zoom Out**, or click the Zoom Out icon in the Net Map task bar. Each time you click **Zoom Out**, Net Map zooms out one level and the Zoom Controller is updated accordingly.

**Net Map Tasks**

From Net Map, you can create IPv4 networks, and evaluate and manage your network resources according to the needs of your organization.

You can do the following:

- **Zoom in on specific areas, as described in Zooming In and Out.**
- **Add a network, as described in Adding a Network from Net Map.**
- **Select a network and view either its network or Net Map, as described in Viewing Network Details.**
- **Select a network and edit its properties, as described in Modifying IPv4 and IPv6 Network Containers and Networks.**
- **Split a network, as described in Splitting IPv4 Networks into Subnets.**
- **Join networks, as described in Joining IPv4 Networks.**
- **Resize a network, as described in Resizing IPv4 Networks.**
- **(Applies only with Network Insight) Execute vDiscovery on the selected network, as described in Configuring vDiscovery Jobs.**
- **(Applies only with Network Insight) View Discovery Status for the selected network, as described in Viewing Discovery Status.**
- **(Applies only with Network Insight) Execute Discovery Diagnostics on the selected network, as described in Executing Discovery Diagnostics.**
- **(Applies only with Network Insight) Direct NIOS to discover devices on the selected network (Discover Now).** The network must have discovery enabled before this button will be active. For more information about requirements and discovery features, see the topics under About Network Insight.

**Note:** If the Discover Now button and other associated discovery elements are disabled on the Toolbar, it indicates that discovery is not enabled for the parent network of the selected network or IP, or the network is not associated with a discovery appliance.

**Delete one or multiple networks, as described in Discovering Networks (Under Network Insight only).**

- **Clear All Unmanaged Data or Clear All Discovered Data, as described in the section Clearing Discovered Data.**
- **Switch to the List view of the network. For information, see IPAM Home.**
  - When you select one or more networks in the List view and then switch to the List view, the list displays the page with the first selected network.
  - If you select one or more networks in the List view and then switch to the Net Map view, the first network is also selected in Net Map. If you select a network in the List view that is part of a Multiple Networks block in Net Map, it is not selected when you switch to the Net Map view.

**Adding a Network from Net Map**

When you create networks from Net Map, you can evaluate your network infrastructure and add networks accordingly. You can view the address space to which you are adding a network, so you can determine how much space is available and which IP addresses are not in use. When you mouse over an open area, Net Map displays useful information, such as the largest possible network that fits in that area and the total number of IP addresses. In addition, you can create networks without having to calculate anything. When you add a network, Net Map displays a netmask slider so you can determine the appropriate netmask for the size of the network that you need. As you move the slider, it displays network information, including the total number of addresses. After you select the netmask, you can even move the new network around the open area to select another valid start address.

To add a network from the Net Map panel:

1. Do one of the following:
   - Click the Add icon.
   - Net Map displays the netmask slider and outlines the open area that can accommodate the largest network.
   - Select an open area, and then click the Add icon.
     - Net Map displays the netmask slider and outlines the largest network that you can create in the open area that you selected.

2. Move the slider to the desired netmask. You can move the slider to the netmask of the largest network that can be created in the open area.
   - As you move the slider, Net Map displays the netmask and its corresponding number of IP addresses. The outline in the network map...
also adjusts as you move the slider. When you mouse over the outline, it displays the start and end address of the network.

3. After you set the slider to the desired netmask, you can drag the new network block around the open area to select a new valid starting address. You cannot move the block to a starting address that is invalid.

4. Click Launch Wizard to create the network.

The Add Network wizard displays the selected network address and netmask.

5. You can add comments, automatically create reverse mapping zones, and edit the extensible attributes. (For information, see Adding IPv4 Networks.) You cannot change the network address and netmask.

6. Save the configuration and click Restart if it appears at the top of the screen. Grid Manager updates Net Map with the newly created network.

Viewing Network Details

From the Net Map panel, you can focus on a specific network or area and view additional information about it. If you have a network hierarchy of networks within network containers, you can drill down to individual leaf networks and view their IP address usage.

1. Select a network or area.
2. Click the Open icon.
   - If you selected a network container, Grid Manager displays it in the Net Map panel. You can drill down further by selecting a network or open area and clicking the Open icon again.
   - If you selected a block of multiple networks, Grid Manager displays the individual networks in the Net Map panel. You can then select a network or open area for viewing.
   - If you selected a leaf network, Grid Manager displays it in the IP Map panel.
   - If you selected an open area, Grid Manager displays an enlarged view of that area in the Net Map panel.

This is useful when you are creating small networks in an open area.

IPAM Home

The IPAM Home panel is an alternative view of an IPv4 and IPv6 network hierarchy. For a given network, the panel shows all the networks of a selected network view in table format. This panel displays only the first-level subnets. It does not show further descendant or child subnets. You can open a subnet to view its child subnets. Subnets that contain child subnets are displayed as network containers. If the number of subnets in a network exceeds the maximum page size of the table, the network list displays the subnets on multiple pages. You can use the page navigation buttons at the bottom of the table to navigate through the pages of subnets.

The IPAM home panel displays the following:

- **Network**: The network address.
- **Comment**: The information you entered about the network.
- **RIROrganization**: This appears only if support for RIR updates is enabled. This displays the name of the RIR organization to which the network is assigned.
- **RIROrganizationID**: This appears only if support for RIR updates is enabled. This displays the ID of the RIR organization to which the network is assigned.
- **RIRRegistrationStatus**: This appears only if support for RIR update is enabled. This field displays the RIR registration status. This can be Registered or NotRegistered. Registered indicates that the network has a corresponding entry in the RIPE database.
- **LastRegistrationUpdated**: Displays the timestamp when the last registration was updated. The displayed timestamp reflects the timestamp used on the Grid Master.
- **StatusOfLastRegistrationUpdate**: Displays the registration status and communication method of the last registration update. The status can be Pending, Sent, Succeeded, or Failed. Each time you send a registration update to create, modify, or delete a network container or network, the updated status will be displayed here. If you have selected not to send registration updates, the previous status is retained.
- **IPAMUtilization**: For a network, this is the percentage based on the IP addresses in use divided by the total addresses in the network.

For example, in a /24 network, if there are 25 static IP addresses defined and a DHCP range that includes 100 addresses, the total number of IP addresses in use is 125. Of the possible 256 addresses in the network, the IPAM utilization is about 50% for this network.

For a network container that contains subnets, this is the percentage of the total address space defined within the container regardless of whether any of the IP addresses in the subnets are in use. For example, when you define a /16 network and then 64 /24 networks underneath it, the /16 network container is considered 25% utilized even when none of the IP addresses in the /24 networks is in use.

You can use this information to verify if there is a sufficient number of available addresses in a network. The appliance updates the IPAM utilization data immediately for a network container, but for a network it is updated every 15 minutes.

The IPAM utilization data is displayed in one of the following colors:

- **Red**: The IPAM utilization percentage is above the configured Trigger value.
- **Blue**: The IPAM utilization percentage is below the configured Trigger value.
- **Active Users**: The number of active users on the selected network.
- **Discovery Engine**: Displays the discovery engine that performs the discovery process. This can be NetworkInsight, NetMRI, or vDiscovery. This field displays None if you have added or imported the network container or network manually.
- **Site**: The site to which the IP address belongs. This is a predefined extensible attribute.
- **Bridge Domain**: The name of the discovered bridge domain. This column will display values only for IP addresses that are discovered from Cisco APIC by Network Insight or NetMRI. If discovered by NetMRI, the value will be populated through IPAM Sync. Otherwise, this column will be blank. For information about how to configure Cisco APIC, see Configuring Cisco Application Policy Infrastructure Controller (APIC).
- **Tenant**: The name of the discovered tenant. This column will display values only for IP addresses that are discovered from Cisco APIC by Network Insight or NetMRI. If discovered by NetMRI, the value will be populated through IPAM Sync. Otherwise, this column will be blank. For information about how to configure Cisco APIC, see Configuring Cisco Application Policy Infrastructure Controller (APIC).
You can select the following columns for display:

- **Disabled**: Indicates whether the network is disabled.
- **Leaf Network**: Indicates whether the network is a leaf network or not. A leaf network is a network that does not contain other networks.
- **Discovery Enabled**: (Applies only with Network Insight) Indicates whether discovery is allowed on the network container or the network.
- **Discover Now**: (Applies only with Network Insight) Indicates when the network is undergoing a current discovery process. A "Pending" icon appears in this column when you start the discovery and displays Completed after the completion of the discovery process.
- **VLAN Name**: (AppliesonlyWithNetworkInsight) The VLAN name on the switch port.
- **VLAN ID**: (AppliesonlyWithNetworkInsight) The VLAN ID on the switch port.
- **Managed**: (AppliesonlyWithNetworkInsight) Indicates whether the network is set to Managed status under Grid Manager. For more information, see the section Converting Unmanaged Networks under IPAM to Managed Status.
- **First Discovered**: (AppliesonlyWithNetworkInsight) The date and timestamp of the first occasion that Grid Manager discovered the network.
- **Last Discovered**: (AppliesonlyWithNetworkInsight) The date and timestamp of the last occasion that Grid Manager performed discovery on the network. The timestamp is updated whenever any new IP from this network is discovered.
- **Extensible attributes and RIR attributes**: You can select the extensible attributes such as Building, Country, Region, State, and VLAN for display. When you enable support for RIR registration updates, you can also select associated RIR attributes for display. For information about RIR attributes, see Managing RIR Attributes.
- **Active Directory Sites**: You can also select Active Directory Sites for display. For information about Active Directory Sites, see About Active Directory Sites and Services.

You can sort the list of networks in ascending or descending order by columns. For information about customizing tables in Grid Manager, see Customizing Tables.

You can also modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.

**Tip:** If you select a network from the list and switch to the Net Map panel, the network is also selected in the network map.

**Filtering the Network List**

You can filter the network list, so it displays only the networks you need. You can filter the list based on certain parameters, such as network addresses, comments and extensible attributes. When you expand the list of available fields you can use for the filter, note that the extensible attributes are those with a gray background.

**Resizing IPv4 Networks**

You can resize a network to increase or decrease the network size and the number of IP addresses in the network. When you resize a network to a smaller netmask, you increase the number of IP addresses within that network. You can change the size of an IPv4 network when the operation does not affect existing objects in the network. You can resize an existing network only if the resized network does not exceed the upper network limit or create orphan objects, such as hosts and DHCP ranges. When a network has a parent network or subnets, the upper limit of the network size is marked in red in the resize network slider, and you cannot resize beyond this limit. For example, if a network has a /16 parent network, you cannot resize the network to a network that is larger than /16.

Before you resize an RIR allocated network block, ensure that the network block has already been registered at the corresponding RIR. Otherwise, when you reassign addresses within this block, the registration updates may fail. For information about RIR registration updates, see RIR Registration Updates.

To resize a network:

1. From the Net Map or List panel, select a network, and then click Resize from the Toolbar.
2. In the Resize Network editor, do the following:
   - **Address**: Displays the network address. You cannot modify this field.
   - **Netmask**: Displays the netmask of the network as you resize the network. You cannot modify this field.
   - **Resize slider**: Use the resize network slider to specify the appropriate subnet masks for the subnets. When you move the slider, Grid Manager displays the number of subnets and IP addresses within that subnet.
   - **Automatically create reverse-mapping zone**: This is enabled only when you resize a /8, /16, or /24 network. Select this check box to have the appliance automatically create reverse-mapping zones for the subnet. The appliance automatically creates reverse-mapping zones only for /8, /16, and /24 netmasks.
3. Click OK.

**Splitting IPv4 Networks into Subnets**

You can create smaller subnets simultaneously within a network by splitting it. You do not have to configure each subnet individually. You can create smaller subnets with larger netmasks. A larger netmask defines more networks with a smaller number of IP addresses. These subnets inherit the address properties of the parent network, such as member assignments. The exceptions are the default router and broadcast address configuration. The default router and broadcast address configuration for address ranges and fixed address are disabled by default after splitting a network. You can enable these properties for each subnet after splitting the parent network.

Note that you cannot split a network that is part of a shared network. To split a network:
1. From the Net Map or List panel, select a network, and then click **Join** from the Toolbar.
2. In the **Join Network** editor, do the following:
   - **Address**: Displays the network address. You cannot modify this field.
   - **Netmask**: Displays the netmask of the network. You cannot modify this field.
   - **Join Network slider**: Use the join network slider to specify available subnet masks for the newly expanded network. Select a smaller netmask value, based on your requirements for the newly-expanded network. When you move the slider, a dialog box displays the total number of IP addresses and the IP address range of a selected subnet mask.
   - **Automatically create reverse-mapping zones**: Select this check box to configure the expanded network to support reverse-mapping zones for the subnets.
3. Click **OK**.

Joining IPv4 Networks

Joining multiple networks into a larger network is the opposite of splitting a network. You can select a network and expand it into a larger network with a smaller netmask. A smaller netmask defines fewer networks while accommodating a larger number of IP addresses. Joining or expanding a network allows you to consolidate all of the adjacent networks into the expanded network. Adjacent networks are all networks falling under the netmask of the newly-expanded network. You can expand the selected network to a new size and add all other subnets into the new network. When you join networks, you need not define all small networks that cover the address spaces for a larger network. Each of the adjacent networks join the expanded network and inherit the DHCP member configuration options of the selected network. The expanded network does not inherit the default router and broadcast address configurations of the adjacent networks. Those configurations are disabled by default.

**Note**: The member assignment for the expanded network combines all member assignments of the joining networks.

Note that the join and resize features work identically only when you have a single network. If the resize feature is disabled and if you have a single network object with additional new networks, then you must use the join feature to combine all networks.

To join or expand a network:

1. From the Net Map or List panel, select a network, and then click **Join** from the Toolbar.
2. In the **Join Network** editor, do the following:
   - **Address**: Displays the network address. You cannot modify this field.
   - **Netmask**: Displays the netmask of the network you are about to expand the network.
   - **Join Network slider**: Use the join network slider to specify the available subnet masks for the newly expanded network. Select a smaller netmask value, based on your requirements for the newly-expanded network. When you move the slider, a dialog box displays the total number of IP addresses and the IP address range of a selected subnet mask.
   - **Automatically create reverse-mapping zones**: Select this check box to configure the expanded network to support reverse-mapping zones for the subnets.
3. Click **OK**.

Discovering Networks (Under Network Insight only)

**Note**: If the **Discover Now** button and other associated discovery elements are disabled on the Toolbar, it indicates that discovery is not enabled for the parent network of the selected network or IP, or that a discovery appliance (known as a Probe) is not associated with the network that you wish to discover.

To discover IPv4 or IPv6 networks:

1. From the Net Map or List panel, select a network, and then click **Discover Now** from the Toolbar. NIOS asks you to confirm that you wish to launch discovery on the selected network.

In the Net Map panel, you can click on IP addresses in the network being discovered. As new data becomes available, NIOS updates the Discovered Data section of the panel with any information found on the device associated with the selected IP.

For more information about requirements and discovery features, see the topics under **About Network Insight**.

Deleting Networks

From the IPAM tab, you can delete multiple IPv4 and IPv6 networks. When you delete a network, all of its data, including all of its DHCP records, subnets, and records in its subnets, is deleted from the database and goes to the Recycle Bin, if enabled. Because of the potentially large loss of data that can occur when you delete a network, Grid Manager requires a confirmation to move the data to the Recycle Bin.

To delete IPv4 or IPv6 networks:

1. From the **Data Management** tab, select the **IPAM** tab -> **network** check box. You can select multiple check boxes for multiple networks.
2. Select **Delete** or **Schedule Delete** from the Delete drop-down menu.
3. To delete the network now, in the **Delete Confirmation** dialog box, click **Yes**. To schedule a deletion, see **About Extensible Attributes**. The appliance puts the deleted network in the Recycle Bin, if enabled.

### Viewing and Managing IPv4 Addresses

You can view and manage IPv4 address data in the IP Map and IP List panels. Grid Manager displays the IP Map and List panels for a specific network after you navigate through the network hierarchy, or when the selected network does not have subnets under it.

### IP Map

The IPv4 Map panel provides a graphical representation of all IPv4 addresses in a given subnet. IP Map displays cells that represent IPv4 addresses. Each cell in the map represents an IPv4 address, and its color indicates its status as described in the legend section. You can run a network discovery on the selected network, and the status of each IP address is updated accordingly. For information, see Chapter 14, *IP Discovery and vDiscovery*.

Each IP Map panel can accommodate up to 256 cells with each cell representing an IP address. If a given network has more than 256 addresses, additional IP addresses are displayed by paging to the next page. You can use the page navigation buttons to page through the IP addresses. To go to a specific IP address, you can enter the IP address in the **Go to** field or click a specific cell in IP Map. IP Map has a basic and an advanced view. You can toggle between these views by clicking **Toggle Basic View** or **Toggle Advanced View**. As illustrated in Figure 13.7, the status of an IP address is represented with a different color in the IP Map panel.

In the basic view, the IP Map panel displays the following IP address status:

- **Unused**: An IP address that has not been detected and is not associated with any network device or active host on the network.
- **Conflict**: An IP address that has either a MAC address conflict or a DHCP lease conflict detected through a network discovery.
- **Used**: An IP address that is associated with an active host on the network. It can be a resource record, fixed address, reservation, DHCP lease, or host record.
- **Pending**: An IP address that is associated with a scheduled task or approval workflow, and the associated operation has not been executed yet. This IP address is not considered when using the next available IP address function.
- **Selected IP Address**: The IP address that you selected.
- **DHCP Range**: The IP addresses within a DHCP range in the network. The appliance highlights the cells using a blue background.
- **Reserved Range**: A range of IP addresses that are reserved for statically configured hosts. They are not served as dynamic addresses. You can allocate the next available IP from the reserved range when you create a static host.

**Figure 13.7 IP Map - Advanced View**

In the advanced view, the IP Map panel displays additional status as follows:

- **Unmanaged**: An IP address that has a discovered host, is not previously known to the appliance, and does not have an A record, PTR record, fixed address, host address, lease, or is not within a DHCP range. You can change an unmanaged address to a host, DHCP fixed address, A record, or PTR record. You can also clear an unmanaged address. All existing administrator permissions apply to the unmanaged addresses.
- **Fixed Address/Reservation**: A host that is either a fixed address or reservation.
- **DNS Object**: An object that is configured for DNS usage.
- **Host Not in DNS/DHCP**: An IP address that is associated with a host record, but is not configured for DHCP or DNS services.
- **Active Lease**: An IP Address that has an active DHCP lease.
- **DHCP Exclusion Range**: A range of IP addresses within a DHCP range. The appliance cannot assign addresses in the exclusion range.
to a client. You can use these addresses as static IP addresses. This prevents address conflicts between statically configured devices and dynamically configured devices.

**Note:** For a Microsoft split-scope range, the appliance highlights the cells using a combination of orange and pink background colors when the network is managed by two Microsoft servers. For a DHCP exclusion range, the appliance highlights the cells using an orange background.

Under the IP map, Grid Manager displays the following information for the IP address that you have selected in the map:

- **Type:** The object type that is associated with the IP address. For example, this can be **Lease, IPv4 DHCP Range** or **Fixed Address**.
- **Comment:** Additional information about the IP address.
- **Lease State:** The lease state of the IP address. This can be one of the following: **Free, Backup, Active, Expired, Released, Abandoned, Reset, Bootp, Static, Offered, or Declined.**
- **Name:** The name of the object type associated with the IP address. This field displays the name of the object type in the native character set if a host record contains IDs. If a host record contains IDs in punycode, this field displays the name in the punycode representation. For example, if the IP address belongs to a host record, this field displays the hostname. For IDs, this field displays the name in the native character set. If punycode is used, then the appliance displays name in punycode.
- **MAC Address:** The discovered MAC address of the host. This is the unique identifier of a network device. The discovery acquires the MAC address for hosts that are located on the same network as the Grid member that is running the discovery. This can also be the MAC address of a virtual entity on a specified vSphere server. The appliance displays an X mark beside the MAC address if it is invalid. For more information about invalid MAC addresses, see **Synchronizing IP Addresses with Invalid MAC Addresses.**
- **DHCP Fingerprint:** The name of the DHCP fingerprint or vendor ID of the network device that was identified through DHCP fingerprint detection. This field displays **No Match** for devices that do not have any DHCP fingerprint information. For information about DHCP fingerprints, see **DHCP Fingerprint Detection.**

You can do the following in the IP Map panel:

- Click **Go to DHCP View** to view DHCP properties of a selected network.
- Select an address range by clicking once on a start address and then use SHIFT+click on the end address. Click **Add -> Range** from the Toolbar to add the selected range as an IPv4 or IPv6 DHCP range or reserved range.
- Click the Resolve Conflict icon to resolve IP address conflicts. For information, see **Resolving Conflicting Addresses.**
- Click the Ping icon to ping a selected IP address. For information, see **Pinging IP Addresses.**
- Click the Reclaim icon to reclaim an IP address. For information, see **Reclaiming Objects Associated with IPv4 and IPv6 Addresses.**
- Click the Clear icon to clear an active lease. For information, see **Clearing Active DHCP Leases.** You can also select an IP address from the IP Map panel and view the following information:
  - General information, as described in **IP Address Header Panel.**
  - Data retrieved through a network discovery or integrated from a PortIQ appliance and Trinzic Network Automation. For information, see **Viewing Discovered Data.**
  - The records associated with the IP address, as described in **Related Objects.**
  - The audit history, as described in **Audit History.**
  - Detailed lease information, as described in **Viewing Detailed Lease Information.**
  - Click **DHCP View** to view DHCP properties of the selected network. For information, see **Modifying IPv4 Networks.**
  - View active network users, as described in **Viewing Active Network Users.**

**IP Address List**

The IP address list panel displays all IPv4 addresses of a selected subnet in table format. The list provides information about the IP addresses in a hierarchy view. You can use this list to view detailed information about each IP address and its related objects in a selected network. This list provides information such as address status, object type, and usage.

You can configure filter criteria to display only IP addresses that you want to see in the table. For example, you can enter "MAC Address begins 00" as the filter criteria to view only IP addresses that have associated MAC addresses that begin with 00. You can also enter a specific IP address in the Go to field to view information about the address.

Grid Manager can display the following information for the IP addresses. You can edit the columns to display information that is not shown by default.

- **IP Address:** The IP address of the corresponding record. The appliance highlights disabled DHCP objects in gray. A DHCP object can be an DHCP address range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address.
- **Name:** The name of the object type associated with the IP address. For example, if the IP address belongs to a host record, this field displays the hostname.
- **MAC Address:** The discovered MAC address of the host. This is the unique identifier of a network device. The discovery acquires the MAC address for hosts that are located on the same network as the Grid member that is running the discovery. This can also be the MAC address of a virtual entity on a specified vSphere server.
- **Bridge Domain:** The name of the discovered bridge domain. This column will display values only for IP addresses that are discovered from Cisco APIC through Network Insight or NetMRI. If discovered by NetMRI, the value will be populated through IPAM Sync. Otherwise, this column will be blank. For information about how to configure Cisco APIC, see **Configuring Cisco Application Policy Infrastructure Controller (API).**
- **Tenant:** The name of the discovered tenant. This column will display values only for IP addresses that are discovered from Cisco APIC through Network Insight or NetMRI. If discovered by NetMRI, the value will be populated through IPAM Sync. Otherwise, this column will be blank. For information about how to configure Cisco APIC, see **Configuring Cisco Application Policy Infrastructure Controller (API).**
- **EPG:** The name of the end point group. This column will display values only for IP addresses that are discovered from Cisco APIC.
through Network Insight or NetMRI. If discovered by NetMRI, the value will be populated through IPAM Sync. Otherwise, this column will be blank. For information about how to configure Cisco APIC, see Configuring Cisco Application Policy Infrastructure Controller (APIC).

- **DHCP Client Identifier**: For an IPv4 address, the DHCP Unique Identifier of the host.
- **Port Reservation**: Lists any Port Reservation from Network Insight that is associated with the IP address. The information takes the form of `device name:interface name`.
- **VIP**: Indicates when the IP address is operating as a Virtual IP and operates in router redundancy.
- **Status**: The current status of the corresponding record. This can be **Used** or **Unused**.
- **Type**: The object type that is associated with the IP address. For example, this can be **Broadcast**, **Lease**, IPv4 **DHCP Range** or **Fixed Address**.
- **Discover Now**: Indicates when the network is undergoing a current discovery process. A “Pending” icon appears in this column when you start the discovery and displays **Completed** after the completion of the discovery process.
- **Usage**: Indicates whether the IP address is configured for DNS or DHCP.
- **Lease State**: The lease state of the IP address. This can be one of the following: **Free**, **Backup**, **Active**, **Expired**, **Released**, **Abandoned**, **Reset**, **BootP**, **Static**, **Offered**, or **Declined**.
- **User Name**: The name of the user who received the lease for the IP address.
- **Task Name**: The name of the task that collected the discovered data. It is usually the ID or task name that collected the data. It is defined on the corresponding Trinzic Network Automation appliance when you import the discovered data to the NIOS appliance. The task name should be defined in the vDiscovery task manager for vDiscovery.
- **Comment**: Additional information about the IP address.
- **First Discovered**: The timestamp when the IP address was initially discovered. This data is read-only.
- **Last Discovered**: The timestamp when the IP address was last discovered. This data is read-only.
- **OS**: The operating system of the discovered host. The OS value can be one of the following:
  - **Microsoft** for all discovered hosts that have a non-null value in the MAC addresses using the NetBIOS discovery method.
  - A value that a TCP discovery returns.
  - The OS of a virtual entity on a vSphere server.
  Note that this field sometimes displays the percentage of certainty about the discovered OS.
  - **NetBIOS Name**: The returned NetBIOS name from the last discovery.
  - **Device Type(s)**: The type of device associated with the IP address, if any: Router, Switch-Router, and other types.
  - **Open Port(s)**: Lists any TCP/UDP ports that are open on the current IP address.
  - **Discover Name**: The name of the discovered IP address, if any was previously assigned by an administrator.
  - **Discover**: The identity of the device that discovered the IP address. The device type for the neighboring device: **Router**, **Switch-Router**, and other types.
  - **Fingerprint**: The name of the DHCP fingerprint or vendor ID of the network device that was identified through DHCP fingerprint detection. This field displays **No Match** for devices that do not have any DHCP fingerprint information. For information about DHCP fingerprints, see DHCP Fingerprint Detection 9.
  - **Site**: The site to which the IP address belongs. This is a predefined extensible attribute.
  - **Disabled** (hidden): Indicates whether the DHCP or DNS record is disabled.

**Note**: For an IP address that falls within a DHCP range, Grid Manager displays extensible attribute values for the DHCP range and fixed address or host record. When you view the same IP address in the DHCP tab however, Grid Manager displays only the extensible attribute values associated with the fixed address or host record, but not the DHCP range. For example, when you define extensible attribute **State** with the value California for DHCP range 1.0.0.1 – 1.0.0.5, and then define extensible attribute **State** with the value Alaska for fixed address 1.0.0.3, Grid Manager displays both California and Alaska in the **State** field for IP address 1.0.0.3 in the IP Address List view. However, when you view 1.0.0.3 from the DHCP tab, the **State** field displays Alaska only.

**IP List Neighbor Information**

Other values will be available for display in the **List** page. Most of the hidden columns consist of information discovered by Grid Manager, to identify devices connected to the network interfaces neighboring the listed IP addresses in the table. These data columns are hidden and must be selected for display by the operator by selecting the **Visible** check box for each field when editing the columns for the table. (Most of this information will not appear unless a device is recognized in IPAM or is in managed state under IPAM.) Additional values include:

- **Discovered Name**: The discovered name of the device bound to the IP address. The IP address may be just one of several or many IP addresses bound to the device on a specific interface.
- **Discovered MAC Address**: The discovered MAC of the interface bound to the IP address.
- **Discover**: Name of the Infoblox appliance that discovered the IP address and its associated information.
- **Attached Device Description**: Listing of the device neighboring to the IP address.
- **Attached Device Address**: The IP address of the neighboring device to the current IP.
- **Attached Device Name**: The name of the device discovered as neighboring to the current IP.
- **Attached Device Vendor**: The device vendor for the neighbor to the current IP address.
- **Attached Device Model**: The device vendor's model number for the neighbor to the current IP address.
- **Attached Device Port Description**: An admin-provided description for the neighboring IP address, if any is discovered.
- **Attached Device Port Name**: The standard port name for the interface facing the current IP address.
- **Attached Device Port**: The neighboring device's connected port number.
- **Attached Device Type**: Indicates the device type for the neighboring device: **Router**, **Switch-Router**, **Switch**, and other types.
- **Port Duplex**: Discovered Duplex setting for the neighboring port, when applicable.
- **Port Link**: Indicates the state of the link: **Connected** or **Disconnected**.
- **Port Speed**: Indicates the speed of the network connection.
Using the List Panel Action Menu

The IP address List panel provides an Action icon column with a series of menu options for features related to IP address management and IP data management under IPAM. Menu choices change based upon the context and the current state of IP addresses in the table; features available in the List panel action menu include the following:

- (Applies only with Network Insight) View Router Redundancy information for discovered IP addresses in an IPv4 network. For active VIPs, you will see several sets of related information:

  - **Active**: lists the active interface in the redundancy pair;
  - **VIP**: The Virtual IP for the router redundancy pair;
  - **Standby**: The standby IP interface for the router redundancy.

Discovery of all three components of the Router Redundancy instance also provides related information for all three IP entities:

- **Show IPAM Address**: opens the IPAM page to the listed IP address;
- **VIP**: Opens the virtual interface in the host device's Interfaces page;
- **Associated router**: The third item lists the hostname router for each of the three IP address entities comprising the redundancy instance. The currently active router will be identified with the Active and VIP objects; the second Standby router is identified with the Standby IP address.

- **Show Interfaces View**: Opens the IP address' related Interface page to highlight the interface's listed information in the table.
- **Assets View → Show Assets**: Opens the IP address's list of network assets that are connected to the IP address or reachable through the IP address in some way, such as through a routable path. Provides a quick look at basic connectivity provided by the selected IP address; for more information about Assets views, see Viewing Assets Associated with Discovered Devices.
- **Clear**: Allows you to remove data associated with the currently selected IP address, form three categories:
  - **Clear Lease**: If the IP interface gets its configuration from a DHCP lease, choosing this option will clear the IP’s DHCP configuration. Applies only to IP addresses that are fully managed through IPAM;
  - **Clear Unmanaged Data**: Clears the discovered data for an unmanaged IP address;
  - **Clear Discovered Data**: Clears discovered data from the IPAM object, and re-launches discovery afterwards if necessary.
- **Convert**: Conversion feature to convert the currently unmanaged IP address to an object fully managed by IPAM: Network, To Host, To A Record, To PTR Record, or To Fixed Address. (For related information, see Managing Discovered Data, About Host Records, Managing A Records and Managing PTR Records.)
- **Discover Now**: Requests Grid Manager to execute discovery on the selected IP address.
- **Exclusion**: Exclude or disable exclusion of the current IP address from discovery. For related information, see Excluding IP Addresses from Discovery.
- **Show Active Users**: Displays all the users who are currently active on the selected network. For information, see Viewing Active Network Users.

Additional IP List Information

You can display all available extensible attributes. You can also sort the list of IP addresses in ascending or descending order by IP Address only. If you enabled the IP Discovery feature, you can configure the IP List panel to display discovered data and fields imported from NetMRI appliances. For information about integrating discovered data from NetMRI, see Integrating Discovered Data From NetMRI.

You can select an IP address from the List panel and view the following information about it:

- General information, as described in IP Address Header Panel.
- Data retrieved through a network discovery or integrated from a PortIQ appliance, as described in Viewing Discovered Data.
- The records associated with the IP address, as described in Related Objects.
- Audit history, as described in Audit History.
- Detailed lease information, as described in Viewing Detailed Lease Information.

You can also do the following from the IP List panel:

- Click Go to DHCP View to view DHCP properties of a selected network. For information, see Modifying IPv4 Networks.
- Click the Ping icon to ping a selected IP address. For information, see Pinging IP Addresses.

Filtering the IP Address List

You can filter the IP address list, so it displays only the IP addresses you need. You can filter the list based on any combination of extensible attributes and the parameters displayed in the IP address list, such as usage and type. When you expand the list of available fields you can add to the filter, note that the extensible attributes are those with the gray background.
IP Address Header Panel

When you select an IP address from the IP Map or List panel, Grid Manager displays information about the highest priority object associated with the IP address. Depending on the object type, Grid Manager displays all or some of the following information. For example, if the highest priority object is a fixed address, Grid Manager displays only the object type, MAC address, lease state, and comment of the object.

- **Type**: The object or record type, such as A record, PTR record, or host record.
- **Name**: The name of the object. For example, if the IP address belongs to a host record, this field displays the hostname. The appliance highlights disabled DHCP objects in gray. A DHCP object can be a DHCP address range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address.
- **MAC**: The MAC address of the network device associated with the IP address.
- **Lease State**: The current status of the DHCP lease.
- **Comment**: Comments about the IP address.

Discovered Data

The **Discovered Data** tab displays discovered data through a network discovery or integrated from PortIQ and NetMRI appliances. For information about viewing discovered data, see Viewing Discovered Data.

Related Objects

The Related Objects tab displays the following information about the records associated with the IP address:

- **Name**: The name of the object. For example, if the IP address belongs to a host record, this field displays the hostname. The appliance highlights disabled DHCP objects in gray. A DHCP object can be a DHCP range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address.
- **Type**: The object type, such as DHCP lease, host, A record, and bulk host.
- **Comment**: Information about the object. You can also select the following for display:
  - **DNS view**: The DNS view to which the object belongs. You can do the following in this tab:
    - Add a resource record. You can select the following from the drop-down list:
      - **Host Record**—For information, see Adding Host Records.
      - **Range**—For information, see Adding IPv4 Address Ranges.
      - **Fixed Address**—For information, see Adding IPv4 Fixed Addresses.
      - **Reservation**—For information, see Adding IPv4 Reservations.
      - **A Record**—For information, see Adding A Records.
      - **PTR Record**—For information, see Adding PTR Records.
    - Edit the properties of the selected object. Depending on the type of object, Grid Manager displays the corresponding editor for the object. For example, if the selected object is a fixed address, Grid Manager displays the fixed address editor. When you select a lease object, Grid Manager displays the lease viewer.
    - You can also modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables. Delete a selected object or multiple objects.
    - When you select a lease object and click the Show Details icon, you can view the lease start and end dates.
    - Depending on the object type, you can convert a selected object to one of the following:
      - **Reservation**
      - **Host**
      - **Fixed Address**
  - Add a resource record. You can select the following from the drop-down list:
    - **Host Record**—For information, see Adding Host Records.
    - **Range**—For information, see Adding IPv4 Address Ranges.
    - **Fixed Address**—For information, see Adding IPv4 Fixed Addresses.
    - **Reservation**—For information, see Adding IPv4 Reservations.
    - **A Record**—For information, see Adding A Records.
    - **PTR Record**—For information, see Adding PTR Records.

Audit History

By default, the Audit History tab displays the following information about the last five actions performed on the selected IP:

- **Timestamp**: The day, date, and time of the operation.
- **Action**: The type of operation that was performed by the administrator.
- **Object Type**: The object type of the entry.
- **Object Name**: The name of the object.
- **Admin Name**: The name of the administrator who performed the operation.
- **Message**: The description of the administrative activity.

**Note**: If you change the IP address of an existing record to a new one in the IP Map tab when the Grid Audit Logging is set to Brief, then NIOS will not display modification or transition details about the new IP address in this tab. You can only view subsequent modifications and deletions to the new IP address. However, you can view the audit log history and transition details of the old IP address, but you cannot view the initial transition from an old IP address to the new IP address.
Managing IPv4 Addresses

You can do the following from the IP Map and List panels:

- Add IP addresses to existing hosts. For information, see Adding IP Addresses to Existing Host Records.
- Clear unmanaged IP addresses. For information, see Clearing Unmanaged Data.
- Convert objects to other object types. For information, see Converting Objects Associated with IPv4 Addresses.
- Reclaim IP addresses. For information, see Reclaiming Objects Associated with IPv4 and IPv6 Addresses.
- Ping IP addresses. For information, see Ping IP Addresses.
- Configure and run a network discovery. For information, see IP Discovery and vDiscovery.
- Resolve discovery conflicts. For information, see Resolving Conflicting Addresses.
- Clear discovered data. For information, see Clearing Discovered Data.

Adding IP Addresses to Existing Host Records

You can add unused and unmanaged addresses, including all their information, to existing host records. When you add an unmanaged address to a host record, the appliance adds the discovered data to the host record. You can select the desired host to which you want to add the unmanaged address.

To add an unmanaged IP address to an existing host record:

1. From the IP Map or List panel, select an IP address, and then click Add -> Add to Existing Host from the Toolbar.
2. In the Select Host dialog box, do the following:
   - In the table, select the host to which you want to add the selected IP address. You can also use the filters or the Go To field to narrow down the host list. For information, see Using Filters and Using the Go To Function.
   - Click the Select icon.
   - Grid Manager displays the Host Record editor.
3. In the Host Record editor, update the host properties as described in Choose one of the following from the Save & ... drop-down button menu.
4. Save the configuration and click Restart if it appears at the top of the screen. To close the editor without saving the changes, click the Close icon.

Clearing Unmanaged Data

You can clear the status of unmanaged data at the network and IP address levels. When you clear an unmanaged address, the status of the IP address changes to Unused. An unmanaged address is an IP address with a discovered host, is not previously known to the appliance, and does not have an A record, PTR record, fixed address, host address, lease, or is not within a DHCP range. You can change an unmanaged address to a host, a DHCP fixed address, an A record, or a PTR record. You can also clear the unmanaged data associated with the address.

To clear unmanaged data:

1. From the IP Map or List panel, select the IP address for which you want to clear unmanaged data, and then click Clear -> Clear Unmanaged Data from the Toolbar. You can select multiple IP addresses.
2. In the Clear Unmanaged data dialog box, click Yes.

Viewing Router Redundancy Information for Virtual IPs (VIPs)

1. From the Data Management tab, click CSV Job Manager from the Toolbar.
2. In CSV Job Manager, click the CSV Import tab and select the import job that you want to delete. Click the Action icon
   and select Delete or click the Delete pending job icon.

Managing IPv6 Networks

In Grid Manager, you can use the IPv6 Net Map (network map) and List panels to manage your IPv6 network infrastructure. After you select a network container from the IPAM tab, Grid Manager displays it in the Net Map panel, by default. The Net Map panel provides a graphical view of your networks and has a number of features that simplify network management. The List panel displays the networks in table format.

You can always switch your view of a network container between the Net Map and List panels. Grid Manager keeps track of which panel you last viewed. After you select a network container, Grid Manager displays it in the Net Map or List panel, depending on which one you last used. For information about each panel, see IPv4 Network Map and IPAM Home.

You can use Grid Manager to manage IPv6 networks and their AAAA, PTR and host resource records. You can configure IPv6 networks and track IP address usage in those networks. You can also split and join IPv6 networks, when necessary.

IPv6 Network Map

After you select an IPv6 network container from the IPAM tab, Grid Manager displays it in the IPv6 Net Map (network map) panel, by default. Just like the IPv4 Net Map, the IPv6 Net Map provides a high-level view of the network address space. You can use Net Map to design and plan your network infrastructure, and to configure and manage individual networks.
The Net Map panel presents a complete view of the network space, including the different types of networks that are in it and its unused address space. IP addresses that belong to a network are blocked off. Each color-coded block represents a network container, a leaf network, or a block of networks that are too small to be displayed individually in the map. For example, in a /64 or /96 network, networks smaller than /76 or /108 respectively and that are beside each other are represented as a multiple network block. In addition, the fill pattern of the blocks indicates their utilization. Therefore, you can quickly evaluate how many networks are in a network container, their relative sizes, utilization, and how much space you have left.

As you mouse over areas of the map, it displays IP information about the area. Net Map also has a zoom feature that allows you to enlarge or reduce your view of a particular area.

Figure 13.9 displays the network map of a 1111::/16 network, which is a network container that has network containers and leaf networks.

**Figure 13.9 IPv6 Network Map**

**Displaying Network Information**

As shown in Figure 13.9, as you mouse over the map, Net Map displays IP information about the area. When you mouse over an unused area, Net Map displays the following information:

- The start and end IP address
- The largest possible network
- The number of /64 networks that can fit in that space

When you mouse over a network container, Net Map displays the following information:

- Network address and netmask
- The first and last IP address of the network
- The number of networks in that block
- IPAM utilization

When you mouse over a network, Net Map displays the following information:

- Network address and netmask
- The first and last IP address of the network
When you mouse over a block of multiple networks, Net Map displays the following information:

- The start and end IP address of that block of networks
- The number of networks in that block

### Zooming In and Out

Use the zoom function to enlarge and reduce your view of a selected area. You can zoom in on any area in your network. You can zoom in on an area until it displays 128 addresses per row, for a total of 1024 addresses for the map. When you reach the last possible zoom level, the Zoom In icon in the Net Map task bar and the menu item are disabled.

After you zoom in on an area, you can click the Zoom Controller icon to track where you zoomed in. The Zoom Controller lists all the areas that you zoomed in and updates its list dynamically. You can click an item on the list to view that area again. Click the Zoom Controller again to close it.

To select an area and zoom in:

1. Right-click and select **Zoom In**, or click the Zoom In icon in the Net Map task bar. The pointer changes to the zoom in selector.
2. Select a starting point and drag to the end point. The starting point can be anywhere in the map. It does not have to be at the beginning of a network.

Net Map displays a magnified view of the selected area after you release the mouse button. As you mouse over the zoomed in area, Net Map displays IP information about it.

3. You can do the following:
   - Select an area and zoom in again.
   - Add a network. If you zoom in on an area and click Add without selecting an open area first, Net Map selects the area where it can create the biggest possible network in that magnified area.
   - Select a network and perform any of the following operations:
     - Edit its properties.
     - Open it to display its IP List.
     - Delete it immediately, or schedule its deletion.
   - Right-click and select **Zoom Out**, or click the Zoom Out icon in the Net Map task bar. Each time you click **Zoom Out**, Net Map zooms out one level and the Zoom Controller is updated accordingly.

### Net Map Tasks

From Net Map, you can create IPv6 networks, and evaluate and manage your network resources according to the needs of your organization.

You can do the following:

- Zoom in on specific areas, as described in **Zooming In and Out**.
- Use the Go to function to find a network in the current zoom level of Net Map.
- Add a network, as described in **Adding a Network from Net Map**.
- Select a network and view IP address list, as described in **Viewing IPv6 Data**.
- Select a network and edit its properties, as described in **Modifying IPv4 and IPv6 Network Containers and Networks**.
- Split a network, as described in **Splitting IPv6 Networks into Subnets**.
- Join networks, as described in **Joining IPv6 Networks**.
- Delete one or multiple networks, as described in **Discovering Networks (Under Network Insight only)**.
- Switch to the List view of the network. For information, see **IPv6 Network List**.
  - When you select one or more networks in Net Map and then switch to the List view, the list displays the page with the first selected network.
  - If you select one or more networks in the List view and then switch to the Net Map view, the first network is also selected in Net Map. Although, if you select a network in the List view that is part of a Multiple Networks block in Net Map, it is not selected when you switch to the Net Map view.

### Adding a Network from Net Map

When you create networks from Net Map, you can view the address space to which you are adding a network, so you can determine how much space is available and which IP addresses are not in use. When you mouse over an open area, Net Map displays useful information, such as the largest possible network that fits in that area. In addition, you can create networks without having to calculate anything. When you add a network, Net Map displays a netmask slider so you can determine the appropriate netmask for the size of the network that you need. As you move the slider, it displays network information, including the total number of addresses. After you select the netmask, you can even move the new network around the open area to select another valid start address.

To add a network from the Net Map panel:

1. Do one of the following:
   - Click the Add icon.
     - Net Map displays the netmask slider and outlines the open area that can accommodate the largest network.
   - Select an open area, and then click the Add icon.
     - Net Map displays the netmask slider and outlines the largest network that you can create in the open area that you selected.
2. Move the slider to the desired netmask. You can move the slider to the netmask of the largest network that can be created in the open area. You can also move the slider to the smallest network that can be placed in the current zoom level of Net Map.

As you move the slider, Net Map displays the netmask. The outline in the network map also adjusts as you move the slider. When you...
mouse over the outline, it displays the start and end address of the network.

3. After you set the slider to the desired netmask, you can drag the new network block around the open area to select a new valid starting address. You cannot move the block to a starting address that is invalid.

4. Click Launch Wizard to create the network.
   The Add Network wizard displays the selected network address and netmask.

5. You can add comments, automatically create reverse mapping zones, and edit the extensible attributes. (For information, see Adding IPv6 Networks.)

6. Save the configuration and click Restart if it appears at the top of the screen. Grid Manager updates Net Map with the newly created network.

Viewing Network Details

From Net Map, you can focus on a specific network or area and view additional information about it. If you have a network hierarchy of networks within network containers, you can drill down to individual leaf networks and view their IP address usage.

1. Select a network or area.
2. Click the Open icon.
   - If you selected a network container, Grid Manager displays it in the Net Map panel. You can drill down further by selecting a network or open area and clicking the Open icon again.
   - If you selected a block of multiple networks, Grid Manager displays the individual networks in the Net Map panel. You can then select a network or open area for viewing.
   - If you selected a leaf network, Grid Manager displays it in the Network List panel.
   - If you selected an open area, Grid Manager displays an enlarged view of that area in the Net Map panel. This is useful when you are creating small networks in an open area.

IPv6 Network List

The Network list panel is an alternative view of an IPv6 network hierarchy. For a given network, the panel shows all the networks of a selected network view in table format. A network list displays only the first-level subnets. It does not show further descendant or child subnets. You can open a subnet to view its child subnets. Subnets that contain child subnets are displayed as network containers. If the number of subnets in a network exceeds the maximum page size of the table, the network list displays the subnets on multiple pages. You can use the page navigation buttons at the bottom of the table to navigate through the pages of subnets.

The IPAM home panel displays the following:

- **Network**: The network address.
- **Comment**: Information you entered about the network.
- **IPAM Utilization**: For a network, this is the percentage based on the IP addresses in use divided by the total addresses in the network. You can use this information to verify if there is a sufficient number of available addresses in a network. The IPAM utilization is calculated approximately every 15 minutes.
- **Site**: The site to which the IP address belongs. This is a predefined extensible attribute.
- **Active Users**: The number of active users on the selected network. You can select the following columns for display:
- **Disabled**: Indicates whether the network is disabled.
- **Leaf Network**: Indicates whether or not the network is a leaf network.
- **Other available extensible attributes

You can sort the list of subnets in ascending or descending order by columns. For information about customizing tables in Grid Manager, see Customizing Tables.

You can also modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.

**Tip**: If you select a network from the list and switch to the Net Map panel, the network is also selected in the network map.

Filtering the Network List

You can filter the network list, so it displays only the networks you need. You can filter the list based on certain parameters, such as network addresses, comments and extensible attributes. When you expand the list of available fields you can use for the filter, note that the extensible attributes are those with a gray background.

Splitting IPv6 Networks into Subnets

You can create smaller subnets simultaneously within a network by splitting it. You do not have to configure each subnet individually. You can create smaller subnets with larger netmasks. A larger netmask defines a larger number of network addresses and a smaller number of IP addresses.

Note that you cannot split a network that is part of a shared network. To split an IPv6 network:

1. From the Data Management tab, select the IPAM tab -> network check box, and then click Split from the Toolbar.
2. In the **Split Network** editor, do the following:
   - **Address**: Displays the network address. You cannot modify this field.
   - **Net mask**: Specify the appropriate netmask for each subnet.
   - **IPv6 Prefix Collector Network**: If you split a network with prefix delegations that are not tied to specific addresses, specify the network in which all prefix delegations are assigned. If you leave this field blank, the server assigns all prefix delegations that are not tied to specific addresses to the first network.
   - **Immediately create**: Select one of the following:
     - **Only networks with ranges and fixed addresses**: Adds only the networks that have DHCP ranges and fixed addresses.
     - **All possible networks**: Adds all networks that are within the selected netmasks. You can select this option only when you increase the CIDR by 8 bits.
   - **Automatically create reverse-mapping zone**: Select this check box to have the appliance automatically create reverse-mapping zones for the subnets. This function is enabled if the netmask of the network is a multiple of four, such as 4, 12, or 16.

3. **Click OK**.

### Joining IPv6 Networks

Joining multiple networks into a larger network is the opposite of splitting a network. You can select a network and expand it into a larger network with a smaller netmask. A smaller netmask defines fewer networks while accommodating a larger number of IP addresses. Joining or expanding a network allows you to consolidate all of the adjacent networks into the expanded network. Adjacent networks are all networks that fall under the netmask of the newly-expanded network.

To join or expand a network:

1. From the **Data Management** tab, select the **IPAM** tab -> **network** check box, and then click **Join** from the Toolbar.
2. In the **Join Network** editor, do the following:
   - **Address**: Displays the network address. You cannot modify this field.
   - **Netmask**: Enter the netmask of the expanded network.
   - **Automatically create reverse-mapping zone**: Select this check box to configure the expanded network to support reverse-mapping zones. The appliance automatically creates reverse-mapping zones only if the netmask is between /4 through /128, in increments of 4 (that is, /4, /8, /12, and so on until /128).
3. **Click OK**.

### Viewing IPv6 Data

To the configured IP addresses in an IPv6 network:

- For a leaf network that is not in a network container, from the **Data Management** tab, select the **IPAM** tab, and then click the IPv6 network you want to view.
- For a leaf network that is in a network container, from the **Data Management** tab, select the **IPAM** tab `network_container -> network`.

Grid Manager lists the configured IPv6 addresses. You can export and print the list. It displays the following information about each IP address:

- **IP Address**: The name of the IPv6 DHCP object, which can be a DHCP range, fixed address, host configured for DHCP, or a roaming host with an allocated IP address.
- **Name**: The name of the record associated with the IP address.
- **DUID**: The DHCP Unique Identifier (DUID) of the device that was assigned the IP address.
- **Status**: The status of the IPv6 object, such as Used or Unused.
- **Type**: The object type associated with the IP address, such as AAAA record, IPv6 Fixed Address, or Unmanaged.
- **Usage**: Indicates whether the IPv6 address is configured for DNS or DHCP.
- **Exclude**: (Applies only with Network Insight) Denotes whether the IP is excluded from discovery.
- **Lease State**: (Applies only with Network Insight) The lease state of the record, such as Active.
- **User Name**: The name of the user who received the lease for the IP address.
- **First Discovered**: (Applies only with Network Insight) The date and timestamp of the first occasion that NIOS discovered the IP address.
- **Last Discovered**: (Applies only with Network Insight) The date and timestamp of the last occasion that NIOS discovered the IP address.
- **OS**: The operating system of the IP.
- **NetBIOS Name**: The returned NetBIOS name from the last discovery.
- **Device Type(s)**: Shows the device type for the device associated with the IP address.
- **Fingerprint**: The name of the DHCP fingerprint or vendor ID of the network device that was identified through DHCP fingerprint detection. This field displays No Match for devices that do not have any DHCP fingerprint information. For information about DHCP fingerprints, see **DHCP Fingerprint Detection**.
- **Comment**: Displays comments about the record.
- **Site**: The site to which the IP address belongs. This is a predefined extensible attribute.

You can display all available extensible attributes. You can also sort the list of IP addresses in ascending or descending order by **IP Address** only.

You can drill down further and view the records associated with an IP address. To view the associated records of an IP address, select it and Grid Manager displays information about the IP address in the **Related Objects** and **Audit History** tabs.
Related Objects
Grid Manager displays the following information about the records associated with the IP address:

- **Name**: The record name. For example, if the IP address belongs to a host record, this field displays the hostname.
- **Type**: The object type. For example, AAAA Record, PTR Record, Host Record, IPv6 Fixed Address.
- **Comment**: Additional information that was entered in the record about the IP address.

Audit History
Grid Manager displays the following information about the last five actions performed on the selected IP:

- **Timestamp**: The day, date, and time of the operation.
- **Action**: The type of operation that was performed by the administrator.
- **Object Type**: The object type of the entry.
- **Admin Name**: The name of the administrator that performed the operation.
- **Message**: Description of the administrative activity.

Filtering the IP Address List
You can filter the IP address list, so it displays only the IP addresses you need. You can filter the list based on any combination of extensible attributes and the parameters displayed in the IP address list, such as usage and type. When you expand the list of available fields you can add to the filter, note that the extensible attributes are those with the gray background.

Managing IPv4 and IPv6 Addresses
Grid Manager uses IP addresses as the entry point to the data set containing Infoblox host, DNS, DHCP, and other information related to that address. You can view the data, modify it, assign extensible attributes to the objects associated with the address, and convert DHCP lease types, such as changing a currently active dynamic lease to a fixed address or host record.

You can view and manage IPv4 address data in the IP Map panel, and view and manage IPv4 and IPv6 data in the IP List panel. You can do the following for IPv4 and IPv6 data from the IP List panel:

- Convert objects to other object types. For information, see [Converting Objects Associated with IP Addresses](#).
- Reclaim IP addresses. For information, see [Reclaiming Objects Associated with IPv4 and IPv6 Addresses](#).
- Ping IP addresses. For information, see [Pinging IP Addresses](#).
- Clear DHCP leases. For information, see [Clearing Active DHCP Leases](#).

You can also print and export in CSV format the information displayed in any panel that supports these functions.

Converting Objects Associated with IP Addresses
The NIOS appliance provides a simple mechanism for converting unmanaged IP addresses to resource records, such as host records and A or AAAA records. You can also convert the active lease of a dynamically assigned IPv4 or IPv6 address to a fixed address or host, and convert an IPv4 lease to an IPv4 reservation. Using the conversion mechanism, you can keep the existing information of a network device during the conversion.

The appliance supports the following conversions for IPv4 objects:

- DHCP leases to fixed addresses, reservations, or host records
- Fixed addresses to reservations or host records
- Unmanaged addresses to host records, A records, PTR records, or fixed addresses
- A records to host records
- PTR records to host records

The appliance supports the following conversions for IPv6 objects:

- DHCP leases to fixed addresses or host records
- Fixed addresses to host records
- AAAA records to host records
- IPv6 PTR records to host records

**Note**: You cannot convert unmanaged IP addresses or leases served by Microsoft DHCP servers to host records.

Converting DHCP Leases
To create a fixed address, you bind an IPv4 address to a MAC address or an IPv6 address to a DUID. You can make that binding by converting an active dynamically leased address to a fixed address. The lease conversion transforms the temporary binding between the IPv4 address and
MAC address or the IPv6 address and DUID in the dynamic lease to a persistent one. The lease must be active so that the NIOS appliance has an IPv4-to-MAC address or IPv6-to-DUID binding to convert into a fixed address. The appliance uses the following rules when converting a DHCP lease:

- If an IPv4 DHCP lease is converted to a fixed address, the appliance copies the client identifier to the fixed address, based on information in the lease. If the appliance finds the client identifier in the lease information, the appliance includes it when it creates the host. If it finds the MAC address, the appliance includes it when it creates the host. If it finds both, the appliance includes only the MAC address (default) when it creates the host.
- If an IPv6 DHCP lease is converted to a fixed address, the appliance copies the DUID to the fixed address.
- If you try to convert an IPv4 DHCP lease or a fixed address with a client identifier, not a MAC address, to a host, the appliance displays an error message in the host editor. This ensures that you do not attempt this operation and lose the data.
- You cannot create two IPv4 fixed addresses with the same client identifier or MAC address in the same network. You cannot create two IPv6 fixed addresses with the same DUID in the same network.
- If the appliance receives a second IPv4 DHCP request with the same client identifier, it provides the same fixed IP address if the lease is still binding.

Figure 13.10 illustrates converting a dynamic IPv4 lease to a fixed lease.

Figure 13.10 Converting a Dynamic IPv4 Lease to a Fixed Lease

![Diagram](image)

An advantage of converting an active dynamic lease is that you do not need to learn the MAC address or DUID of the device to which you want to assign an IP address and manually enter it in the fixed address configuration.

An IPv4 reservation is an address that you exclude from DHCP use because you intend to configure that address manually on a device, such as a firewall, router, or printer. You can also convert an IPv4 fixed address or a dynamic address with an active lease to a reservation. When you convert an address in a DHCP range to a reservation, you reduce the total number of dynamically assignable addresses in that range by one. Correspondingly, this reduces the number of allocated addresses needed to exceed a high or low watermark threshold for that range.

**Note:** To return an IP address to its place in a DHCP range after converting it from an active dynamic lease to a fixed address, reservation, or Infoblox host, delete the fixed address, reservation, or host to which you previously converted the IP address. The IP address then becomes part of the DHCP range to which it first belonged.

You can convert IPv4 fixed addresses to reservations, as shown in Figure 13.11.

Figure 13.11 Converting an IPv4 Dynamic Lease or Fixed Address to a Reservation

DHCP Client and Server Statically Configured Device and DHCP Server
To convert an object:

1. From the IP Map, select an IPv4 address or from the IP List panel, select an IPv4 or IPv6 address.
2. In the Related Objects tab, select the check box of the object, and then click Convert from the Toolbar or navigation bar.
3. Select the object type to which you want to convert the object. Grid Manager displays the corresponding editor for the object type.
4. For all IPv4 conversions, Grid Manager populates the discovered information in the corresponding editor. Depending on the type of conversion, do one of the following:
   - For host record conversions, see Choose one of the following from the Save & ... drop-down button menu:
   - For IPv4 reservation conversions, see Modifying IPv4 Reservations.
   - For fixed address conversions, see Modifying IPv4 Fixed Addresses.
   - For A record conversions, see Modifying A Records.
   - For PTR record conversions, see Modifying PTR Records.

   **Note:** When you select an object for conversion, Grid Manager displays only the available conversion types for the object. You must save the changes in the editor for the conversion to take place.

### Reclaiming Objects Associated with IPv4 and IPv6 Addresses

You can use the reclaim IP function to delete all objects, except the active DHCP lease, that are associated with a selected IP address. To delete a DHCP lease, use the clear lease function as described in Clearing Active DHCP Leases. When you reclaim an IP address, Grid Manager deletes the associated objects and puts them in the Recycle Bin, if enabled. You can reclaim any used and unmanaged IP addresses. You can also select multiple IP addresses for this function. After you reclaim an IP address, the address status changes to Unused. You can then reallocate the IP address to other objects. For example, when you reallocate a fixed address, Grid Manager deletes the fixed address object and puts it in the Recycle Bin. When you reallocate an IP address that is associated with a host record and the address is the only address in the host, Grid Manager deletes the host record.

Grid Manager deletes all the objects that are associated with the selected IP addresses and puts them in the recycle bin, with the following exceptions:

- When you reclaim IP addresses that are in a DHCP range, all the objects that are associated with the IP addresses are deleted and the IP addresses remain in the DHCP range.
- When you select an IP address that is part of a host record, only the selected IP address is deleted from the host. However, if the selected address is the only address in the host, Grid Manager deletes the host record.

Grid Manager does not reclaim the following:

- Unused IP addresses
- Bulk hosts

To reclaim an IP address:

1. From the IP Map or List panel, select the IP address you want to reclaim, and then click Reclaim from the Toolbar. You can select multiple IP addresses.
2. In the Delete Confirmation dialog box, click Yes.

Grid Manager puts the deleted objects in the Recycle Bin, if enabled.

### Pinging IP Addresses

You can find out whether an IP address is accessible and active by pinging the address. Grid Manager sends a packet to the selected IP address and waits for a reply when you ping the address. You can ping individual IP addresses from the IP Map and IP List panels. You can ping all IP addresses from the IP Map panel and all IP addresses on the selected page from the IP List panel.

To ping an IPv4 or IPv6 address:

- From the IP Map or IP List panel, select the IP address that you want to ping, and then click **Ping** from the Toolbar.

To ping all IPv4 addresses:

- From the IP Map panel, click **Multi-ping** from the Toolbar. Grid Manager pings all IP addresses displayed in the IP Map panel and displays the ping status in the panel. When the ping or multi-ping is complete, the status bar displays the number of active IP addresses detected through the ping. To close the ping status bar, click the Close icon.

- From the IP List panel, click **Multi-ping** from the Toolbar. Grid Manager pings all IP addresses visible on the selected page. When the ping or multi-ping is complete, the status bar displays the number of active IP addresses detected on the selected page. To close the ping status bar, click the Close icon.

### Clearing Active DHCP Leases

A DHCP lease specifies the amount of time that the DHCP server grants to a network device the permission to use a particular IP address. You may sometimes need to terminate an active lease. The following are some of the reasons for clearing active DHCP leases:

- When a network device is moved to another network.
- Reset a DHCP lease to fix other problems.

In Grid Manager, you can select multiple IP addresses and clear their active DHCP leases.

To clear an active lease:

1. From the IP Map or List panel, select the IP address for which you want to clear a DHCP lease, and then click **Clear** -> **Clear Lease** from the Toolbar. You can select multiple IP addresses.

2. In the **Clear DHCP Lease Confirmation** dialog box, click Yes.

### Configuring Thresholds for IPAM Utilization

You can define thresholds for IPAM utilization in a network or network container and configure the appliance to send SNMP trap and email notifications to a designated destination when IPAM utilization in a network or network container crosses the configured threshold. IPAM utilization for a network is the percentage based on the IP addresses in use divided by the total addresses in the network and for a network container that contains subnets, it is the percentage of the total address space defined within the container regardless of whether any of the IP addresses in the subnets are in use. The appliance sends an SNMP trap and email notification only once when the IPAM utilization in a network or network container exceeds the Trigger value and when it drops below the Reset value. The default Trigger value is 95% and the default Reset value is 85%. The IPAM utilization notifications are sent for IPv4 networks and IPv4 network containers only. The appliance updates the IPAM utilization data immediately for a network container, but for a network it is updated every 15 minutes.

You can define thresholds for IPAM utilization at the Grid level and network level. The appliance applies the settings hierarchically in a parent-child structure. By defining thresholds at a higher level, all networks can then inherit the same settings and you do not have to redefine them for each network. For example, if you set the thresholds for IPAM utilization at the Grid level, then the settings applies to all the network containers and networks in any network view. However, if you override these settings at the network container or network level, then the settings applies to that network or network container and any network within that network or network container in the same network view. If you set the thresholds for an individual network, then it overrides settings at a higher level.

**Note:** Infoblox recommends that you do not enable SNMP traps and email notifications for IPAM utilization during an upgrade, because if you have configured notifications you may have to unconfigure them during an upgrade.

You can configure the thresholds for IPAM utilization at the Grid level and override them at the network level. To configure the IPAM utilization thresholds at the Grid level, see **Defining Thresholds for Traps**.

To configure the IPAM utilization thresholds for a IPv4 network, network container, or network template, complete the following:

1. **Network Container:** From the Data Management tab, select the IPAM tab -> network_container check box, and click the Edit icon.

   **Network:** From the Data Management tab, select the DHCP tab -> Networks -> network check box, and click the Edit icon.

   **Network Template:** From the Data Management tab, select the DHCP tab -> Templates tab -> DHCP_template check box, and click the Edit icon.

2. In the editor, click **Toggle Advanced Mode**, select the IPv4 IPAM Utilization Notification tab, and then complete the following:
   - **IPAM Utilization Notification:** Click **Override** to override the inherited property, and specify the following:
     - **Enable SNMP Notifications:** Select this for the appliance to send an SNMP trap to the trap receiver that you define for the Grid when IPAM utilization crosses the configured threshold.
You can view all the users who are currently active on a network in the "Active Users" tab. Using the Action icon , you can do the following in the "Active Users" tab:

- **Go To IPAM IP Address Details**: Select this to open the IPAM Home page to view the network address of the device. This option is greyed out for devices that have an IP address and is not part of an IPAM network.
- **Go To DHCP Network Details**: Select this to open the DHCP > Networks tab to view the network address of the device. This option is

### About Network Insight

In some deployments, NIOS IPAM offers network discovery capabilities. NIOS discovery includes Network Discovery and Network Insight, which is a superset of Network Discovery that supports SNMP and enables detailed viewing and assessments of network devices in managed and unmanaged networks, including networks in routed paths, security infrastructure devices, and networks within switched Ethernet segments. Deployment of Network Insight discovery requires a separate Discovery license and one or more NIOS appliances dedicated to discovery tasks. Types of discovered devices include Ethernet switches (including enterprise L3 switches), routers, wireless routers and access points, firewalls, hosts and other devices in end host networks, and much more. Network Insight applies discovery in the following ways:

- Through specification of seed routers, which inform discovery of the various networks that should be examined and catalogued.
- Through discovery of the various Object types you can create under IPAM and DHCP, including IPv4 and IPv6 Networks, Host Records, IPv4 reservations, DHCP ranges, and IPv4/IPv6 fixed addresses.
- An enhanced VM discovery allowing both scheduled VM discovery and immediate discovery of VMs.

For more information about network discovery, see the chapter *IP Discovery and vDiscovery* and its various sections. For a complete discussion of Network Insight, see the chapter *Infoblox Network Insight* and its various sections.

### Viewing Identity Mapping Information

You can view user information associated with networks, end-host devices, Active Directory domains, routers and switches when you enable the Identity Mapping feature on the appliance. Access to user information related to networks and devices help network administrators to understand how the network resources are consumed and by whom. Each network user being mapped can use different devices to access their network environment. So using the identity mapping feature and synchronizing servers, such as Microsoft servers and Cisco ISEs, on the Infoblox appliance provide visibility of user interaction with their environments. By enabling this feature, you can monitor domain users, the IP addresses they log on to, the login status, and the time duration of their current status in the Network tab. For information about Identity Mapping for Active Directory users, see *Configuring Identity Mapping* and how to collect about user and device information from Cisco ISEs, see *Configuring Cisco ISE on NIOS*. You can generate the user login history report to monitor user login activities in a given time frame. For information, see *User Login History Report*.

You can do the following in the Network Users tab:

- View active network users, as described in Viewing Active Network Users.
- View user login history, as described in Viewing Network Users Login History.

### Enabling Identity Mapping

You must first enable the Identity Mapping feature to view user information of a network or device. Complete the following to enable this feature:

1. From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties Editor, select the General tab -> Advanced tab, and then complete the following:

   - **Enable Network Users feature**: Select this check box to enable the Identity Mapping feature on the appliance. Note that the Network Users tab is available only after you enable this feature.

   **Note**: On an Infoblox appliance, the **Enable Network Users Feature** option is disabled by default for all new installations.

3. Save the configuration.

### Viewing Active Network Users

You can view all the users who are currently active on a network in the Active Users tab. Using the Action icon , you can do the following in the Active Users tab:

- **Go To IPAM IP Address Details**: Select this to open the IPAM Home page to view the network address of the device. This option is greyed out for devices that have an IP address and is not part of an IPAM network.
- **Go To DHCP Network Details**: Select this to open the DHCP > Networks tab to view the network address of the device. This option is
greyed out for devices that have an IP address and not managed by the Grid.

- **Go To IPAM Network Details**: Select this to open the IPAM Map for the selected user. The page shows network information in graphical format. This option is greyed out for devices that have an IP and not managed by the Grid.

To view active users:

1. From the **Data Management tab**, select the **Network Users tab** > **Active Users tab**.
   or
   You can use the Action icon
   in the following tabs to open the **Active Users** dialog box:
   - **IPAM tab**: From the **Data Management** tab, select the **IPAM tab**, click the Action icon
   - **DHCP tab**: From the **Data Management** tab, select the **DHCP tab > Networks tab**, click the Action icon
   - **Cloud tab**:
     - In the **Networks tab**, click the Action icon
     - next to the respective network and select **Show Active Users**.
     - **DNS tab**: From the **Data Management** tab, select the **DNS tab > Zones tab > Records tab**, click the Action icon
   - **Active Users** tab: From the **Data Management** tab, select the **VMs tab > Networks tab**, click the Action icon
   - next to the respective network and select **Show Active Users**.

   The **Active Users tab** or **Active Users** dialog box displays the following information:

   - **User Name**: Displays the logon name of the user. When the same user logs in to the domain from multiple clients, entry for each IP address is displayed separately. If multiple users logs in to the same domain, entry for each user is listed separately.
   - **Domain**: The name of the domain.
   - **First Seen**: The timestamp when the user logged in to the network for the first time.
   - **IP Address**: The IP address of the client.
   - **Data Source**: The IP address of the Microsoft server or the API method.
   - **Data Source IP Address**: Displays the source from which the data is collected. It can be Cisco ISE, Microsoft server or the API method.
   - **Status**: The status of the user. The status can be one of the following: **Active** (logged in), **Logged Out**, and **Timed Out**.
     - **Active**: The user is logged in and active.
     - **Logged Out**: The user has logged out of the system.
     - **Timed Out**: The user is logged in but has been idled for a certain period of time. The default is two hours. You can configure this time interval, as described in
   - **Last Seen**: The timestamp when the user was last seen accessing the network.
   - **Last updated**: The timestamp when the user information was last updated.

### Viewing Network Users Login History

You can view the login history of end-host devices, networks, and Active Directory domain users. You must first enable the identity mapping feature to view user login information. For information about enabling Identity Mapping feature, see [Enabling Identity Mapping](#).

To view network user login history:

1. From the **Data Management tab**, select the **Network Users** tab -> **User History** tab. Grid Manager displays the following information:
   - **User Name**: The logon name of the user. When the same user logs in to the Active Directory domain from multiple clients, entry for each IP address is displayed separately. If multiple users logs in to the same Active Directory domain, entry for each user is listed separately.
   - **Domain**: Name of the Active Directory domain.
   - **First Seen**: The timestamp when the user logged in to the Active Directory domain for the first time.
   - **Log Out Time**: Displays the log out time of the user.
   - **IP Address**: The IP address of the client.
   - **Data Source**: The IP address of the Microsoft server or the API method.
   - **Status**: Displays the status of the user. The status can be one of the following: **Active** (logged in), **Logged Out**, and **Timed Out**.
     - **Active**: The user is logged in and active.
     - **Logged Out**: The user has logged out of the system.
     - **Timed Out**: The user is logged in but has been idled for a certain period of time. The default is two hours. You can configured this time interval, as described in
   - **Last Seen**: The timestamp when the user was last seen accessing the network.
   - **Last updated**: The timestamp when the user information was last updated.

### Configuring Active User Timeout Session


You can configure the amount of time that an active session of a user changes to timed out. When the idle session time is reached, the user status changes to inactive status. The default idle time is 2 hours. You can change it to minutes, hours, or days. The user status can be one of the following: Active, Logged Out, and Timed Out.

To configure active user timeout interval:

1. From the Grid tab -> Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit.
2. Select Microsoft Integration tab in the Grid Properties Editor and complete the following in the Basic tab:
   - Assumed Network Users Time Out: Specify the time period after which the user status changes to Timed Out. Select the time period in minutes, hours, or days from the drop-down list.
3. Save the configuration.

Chapter 14 IP Discovery and vDiscovery

This chapter provides information about the Infoblox IP discovery and vDiscovery, and how you can use them to detect, collect, and manage information about active hosts in predefined networks as well as virtual entities in private, public, and hybrid clouds managed through CMPs (Cloud Management Platforms) such as VMware vCenter servers and vSphere Hypervisor, OpenStack, and AWS (Amazon Web Services). It also explains how to integrate and view discovered data from the NetMRI appliances.

This chapter includes the following sections:

- About Discovery
  - Administrative Permissions
  - IP Discovery Process
  - Supported IP Discovery Methods
- Guidelines Before Starting a Discovery
  - Database Updates
  - Database Capacity
  - HA Failover
- Configuring IP Discovery
  - Guidelines for Starting and Scheduling IP Discovery
  - Configuring and Starting an IP discovery
  - Defining IP Discovery Method
  - Scheduling IP Discovery
  - Monitoring IP Discovery Status
- Configuring vDiscovery Jobs
  - Selecting the vDiscovery Member
  - Selecting the Endpoint Server
  - Defining Network Views
  - Defining Policies for Handling Discovered Data
  - Scheduling vDiscovery Jobs
  - Managing vDiscovery Jobs
- Integrating Discovered Data From NetMRI
- Viewing Discovered Data
- Managing Discovered Data
  - Managing Unmanaged Data
  - Resolving Conflicting Addresses
  - Clearing Discovered Data
  - Clearing All Discovery Data

About Discovery

Note: The discovery features described in this chapter apply to NIOS Grid deployments that do not use the Discovery license and its accompanying features under Network Insight. Network Insight provides the ability to discover, query, and catalog routed and switched networks and the devices within them, including infrastructure routers, enterprise switches, security devices such as firewalls, wireless access points, end host computer systems, and more. For more information about Network Insight, see Infoblox Network Insight.

Infoblox provides IP discovery for detecting and obtaining information about active hosts in predefined networks, and vDiscovery for discovering virtual entities and interfaces (such as vSwitch and vRouter) in private, public, and hybrid clouds managed through CMPs (Cloud Management Platforms) such as VMware vCenter servers and vSphere Hypervisor, OpenStack, and AWS (Amazon Web Services). You can configure multiple discovery tasks on one or more discovering members.

- IP discovery: You execute an IP discovery (Data Management tab -> IPAM tab -> Discovery from the Toolbar) to detect active hosts on specified networks in a network view. You can configure the appliance to perform an IP discovery using one of the following protocols: ICMP (Internet Control Message Protocol), NetBIOS (Network Basic Input/Output System), and TCP (Transmission Control Protocol). For more information, see Supported IP Discovery Methods. You can start an IP discovery immediately after you configure it, schedule it for a later date and time, or configure a recurring discovery based on a recurrence pattern. For information about how to configure an IP discovery, see Configuring IP Discovery.
- vDiscovery: This is an extension to the former VM discovery, in which the NIOS appliance only discovers virtual entities on VMware vCenter and vSphere servers. A vDiscovery job (from the Data Management tab -> IPAM tab -> vDiscovery from the Toolbar, or Cloud tab -> any sub tab -> vDiscovery from the Toolbar) now detects virtual entities and interfaces in private, public, and hybrid clouds that are managed through VMware vCenter servers and vSphere Hypervisor, OpenStack, Azure, or AWS. You can define vDiscovery jobs through the vDiscovery Job wizard and manage all configured vDiscovery jobs through the vDiscovery Job Manager. Note that for a
specific vDiscovery job, NIOS synchronizes successive discovered data (not the associated NIOS objects) with the data in the targeted CMP. For example, if you change the IP address of a VM, this information is reflected in the next discovery of the same vDiscovery job. If you terminate a VM, the VM is deleted from the NIOS database. If you delete certain information on the CMP, the respective discovered data is removed from the NIOS database. Be aware that if you change the parameters of a vDiscovery Job, the last discovered data from this job will be automatically cleaned up so that the appliance can continue to synchronize data from one discovery to the next. If you do not want to lose discovered data for a specific vDiscovery Job, you should create a new vDiscovery job for this new collection instead of modifying the current job. For information about how to configure vDiscovery jobs for specific CMPs and how to manage them, see Configuring vDiscovery Jobs and Managing vDiscovery Jobs.

**Note:** For new installations, an IP discovery task is automatically created by default. You can choose to disable the IP discovery after you have set up your appliance. However, you must configure and manually schedule vDiscovery jobs in order for the appliance to detect and collect information about virtual entities in the clouds. When you upgrade from a previous NIOS release to NIOS 7.2 and later, former VM Discovery tasks are divided into separate vDiscovery jobs based on the server endpoints defined in the VM Discovery tasks. All new vDiscovery jobs inherit the same discovery schedule from the old tasks. You must manually enable the new vDiscovery schedules in order for the appliance to perform vDiscovery jobs. For information about how to enable the vDiscovery schedule, see Scheduling vDiscovery Jobs.

After a discovery, the appliance updates the database with the discovered data based on the discovery configuration. For example, you can configure the appliance to merge newly discovered data, consolidate managed data, or update unmanaged data. The appliance also identifies unmanaged and conflict data after a discovery. Unmanaged data is discovered data that is not configured for DNS or DHCP and has no associated NIOS objects. Conflict data is discovered data that is configured for DNS or DHCP and has associated NIOS object or objects, but certain key values are different than those in the NIOS database. For information about guidelines the appliance uses to update discovered data, see Guidelines Before Starting a Discovery and Guidelines for Configuring vDiscovery Jobs.

Grid Manager displays discovered data in the Discovered Data section of the IP address properties panel when you drill down to individual IPs. For information about how to view and manage discovered data, see Viewing Discovered Data and Managing Discovered Data. The appliance records admin operations in the audit log and discovery operations in the syslog. Figure 14.1 shows a high-level perspective of the discovery processes. You can configure and initiate an IP discovery from the Discovery Manage wizard and a vDiscovery from the vDiscovery Job wizard. You must first select a Grid member that runs the discovery tasks. After you configure an IP discovery task and a vDiscovery job, the Grid Master sends the discovery requests to the selected member. Based on the configuration of the discovery tasks, the selected member runs the discovery and collects information about discovered hosts and virtual entities from the specified networks and cloud platforms. The Grid member then reports the discovered results to the Grid Master. Based on the discovery configuration, the Grid Master updates the database with discovered data.

**Administrative Permissions**

You can initiate a discovery and manage discovered data based on your administrative permissions. You must have read/write permission to “Network Discovery” to initiate and manage IP discovery and vDiscovery. You must have at least read-only permission to “All Tenants” and “All Network Views” to view discovered data in the VMs (by IP Address) tab in the Cloud tab. To take actions on discovered data, such as resolving conflicts or clear unmanaged data, you must have read/write permissions. For information about how to configure admin permissions, see About Administrative Permissions.

Following are permission guidelines for initiating and controlling a discovery:

- Superusers can initiate and control a discovery on all networks and CMPs.
- Administrators with read/write permission to “Network Discovery” can initiate and control a vDiscovery job or an IP discovery. For IP discovery, only the objects with IP addresses to which the administrators have read/write permission are updated to include the
discovered data.

After a discovery is completed, the following permission guidelines apply to viewing and managing discovered data:

- Superusers can view and manage all discovered data.
- Administrators with read/write permission to networks can view all discovered data. They can also add unmanaged data to existing hosts, and resolve IP address conflicts.
- Only administrators with read/write permission to a DNS zone or specific record type can convert unmanaged data to a host, fixed address, reservation, A record, or PTR record.
- Administrators with read-only permission to networks can only view discovered data. They cannot change any discovered data.

**IP Discovery Process**

Once an IP discovery starts, the Grid member reports the discovery status, such as **Completed**, **Running**, **Paused**, **Stopped**, or **Error**, in the Discovery Manager wizard and the Discovery Status widget on the Dashboard. In the Discovery Status widget, Grid Manager reports the time when the discovery status was last updated and the numbers of each type of discovered data. For information, see Discovery Status.

When an IP discovery starts, the appliance divides the IP addresses in a network into chunks, with each chunk containing 64 contiguous IP addresses. The discovery process probes each IP address in parallel and in ascending order, reports the detected information, updates the progress report, and then moves on to the next chunk until it hits the last chunk of IP addresses. The appliance then updates the database with the discovered data.

An IP discovery scans the selected networks in the order the networks appear in the Discover Manager wizard.

You can configure discovery processes on the same network, but the same configuration cannot be shared between two discovery processes. Figure 14.2 illustrates how an IP discovery works.

**Figure 14.2 IP Discovery Process**

---

**Supported IP Discovery Methods**

When you perform an IP discovery, you can choose one of the following discovery methods:

- ICMP as described in [ICMP](#).
- NetBIOS as described in [NetBIOS](#).
- TCP as described in [TCP](#).
- Full as described in [Full](#).
These methods actively scan predefined networks and probe IP addresses. The Grid member listens for responses from the IP addresses as proof of activities. The IP discovery scans through the specified network ranges and probes IP addresses (except for the network, broadcast, and multicast address types) in each network, including the /31 and /32 subnets. Note that the possible addresses in the /31 and /32 subnets can be used only as source addresses for point-to-point links. In these cases, there are no broadcast or network addresses in the /31 and /32 subnets, and the appliance can discover source addresses in these subnets.

### ICMP

This method detects active hosts on a network by sending ICMP echo request packets (also referred to as pings) and listening for ICMP echo responses. The ICMP discovery is a simple and fast discovery that detects whether an IP address exists or not. It returns only the IP address and MAC address (only if the Grid member running the discovery is on the same discovered network) of a detected host. The ICMP discovery might miss some active hosts on the network due to security measures that are put in place to block ICMP attacks.

You configure the timeout value and the number of attempts in the **Discovery Manager** wizard. The ICMP discovery method returns the following information for each detected host:

- **IP address**: The IP address of the host.
- **MAC address**: The discovery returns the MAC address only if the Grid member running the discovery is on the same discovered network.

To use the ICMP discovery method, the ICMP protocol between the Grid member performing the discovery and the target networks must be unfiltered.

### NetBIOS

The NetBIOS method queries IP addresses for an existing NetBIOS service. This method detects active hosts by sending NetBIOS queries and listening for NetBIOS replies. It is a fast discovery that focuses on Microsoft hosts or non-Microsoft hosts that run NetBIOS services.

You configure the timeout value and the number of attempts in the **Discovery Manager** wizard. This method returns the following information for each detected host:

- **IP address**: The IP address of the host.
- **MAC address**: Only if the discovered host is running Microsoft.
- **OS**: This value is set to **Microsoft** for an active host that has a MAC address in the NetBIOS reply.
- **NetBIOS name**: This value is set to the name returned in the NetBIOS reply.

To use the NetBIOS discovery method, ports 137 (UDP/TCP) and 139 (UDP/TCP) between the Grid member performing the discovery and the target networks must be unfiltered.

### TCP

The TCP discovery probes each active host on a list of TCP ports using TCP SYN packets. This method detects all active hosts that generate SYN ACK responses to at least one TCP SYN. The discovery can determine the OS on a host by analyzing how the host reacts to the requests on opened and closed ports. It then uses the TCP fingerprints to guess the OS. To obtain a TCP fingerprint, IP discovery provides two scanning techniques, SYN and CONNECT.

When you use the SYN technique, the discovery sends a TCP SYN packet to establish a connection on a TCP port. If the port is open, the host replies with a SYN ACK response. The discovery does not close the port connection.

The CONNECT technique is a three-way TCP handshake. The discovery starts with the same process as the SYN technique by sending the TCP SYN packet. If the host replies with a SYN ACK response, the discovery then sends a RST packet to close the connection. If the response contains a RST flag, it indicates that the port is closed. If there is no reply, the port is considered as filtered. The TCP discovery is a deliberate and accurate discovery method. It can basically detect all active hosts on a network provided that there are no firewalls implemented on the network.

You can select the TCP ports, the TCP scanning technique, and configure the timeout value and the number of attempts in the **Discovery Manager** wizard. This method returns the following information for each detected host:

- **IP address**: The IP address of the host.
- **MAC address**: The discovery returns the MAC address only if the Grid member running the discovery is on the same discovered network.
- **OS**: This is set to the highest probable OS reported in the response.

To use the TCP discovery method, the TCP port and a specific set of ports between the Grid member and the discovered networks must be unfiltered. The default set of ports is defined by the factory settings.

### Full

The full discovery method is a combination of an ICMP discovery, a NetBIOS discovery, a TCP discovery, and a UDP scan. This method starts by sending an ICMP echo request. If no IP address on the network responds to the ICMP request, the discovery ends. If there is at least one response to the ICMP echo request, a NetBIOS discovery starts. A TCP discovery then follows by skipping through the active hosts that the NetBIOS discovery detects. The TCP discovery also handles the NetBIOS-detected hosts that have no MAC addresses. This method also
performs a UDP scan to determine which UDP ports are open. You configure the timeout value and the number of attempts in the Discovery Manager wizard. The full discovery method returns the following information for each detected host:

- IP address
- MAC address
- OS
- NetBIOS name

To use the full discovery, all the filter and firewall requirements in the ICMP, NetBIOS, and TCP discovery methods apply. The following is a summary of the supported IP discovery methods:

<table>
<thead>
<tr>
<th>Discovery Type</th>
<th>Returned Data</th>
<th>Guideline</th>
<th>Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>• IP address</td>
<td>Use ICMP for a rough and fast discovery</td>
<td>ICMP echo request and reply</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetBIOS</td>
<td>• IP address</td>
<td>Use NetBIOS for discovering Microsoft networks or non-Microsoft networks that run some NetBIOS services</td>
<td>NetBIOS query and reply</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NetBIOS name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>• IP address</td>
<td>Use TCP for an accurate but slow discovery</td>
<td>TCP SYN packet and SYN ACK packet</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full</td>
<td>• IP address</td>
<td>Use Full for a general and comprehensive discovery</td>
<td>1. ICMP echo request and reply</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
<td></td>
<td>2. NetBIOS query and reply</td>
</tr>
<tr>
<td></td>
<td>• OS</td>
<td></td>
<td>3. TCP SYN packet and SYN ACK packet</td>
</tr>
<tr>
<td></td>
<td>• NetBIOS name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The method you select to run an IP discovery determines the kind of information the discovery returns and the time it takes to complete an IP discovery. If time is a concern, the following are factors you may consider when configuring an IP discovery:

- The timeout value
- The number of attempts
- The number of ports the discovery scans
- The size of network you want to discover

Guidelines Before Starting a Discovery

Consider the following guidelines before you start a discovery.

Database Updates

After the Grid Master receives discovery data from the Grid member, it integrates the data based on the following rules:

- For a discovered host with a new IP address, the appliance marks the IP address “unmanaged.”
- For a discovered host associated with one of the following, the appliance updates the data of the associated object:
  - A fixed address reservation or host address reservation
  - A host address not configured for DHCP services
  - A fixed address or host address with the same MAC address as that of the discovered host
  - An A or PTR record
  - A DHCP lease with the same MAC address as that of the discovered host
- For a DHCP lease that does not have any associated object, such as a fixed address or host record, the appliance updates the IP address with the discovered data. When the lease expires and the IP address has no associated objects, the appliance marks the IP address “unmanaged”. When the lease expires and the IP address is associated with the same MAC address, the appliance preserves the discovered data.
- For a discovered host associated with one of the following, the appliance updates all data except the MAC address and marks the IP address as a conflict. For information, see Resolving Conflicting Addresses:
  - A fixed address with a different MAC address than that of the discovered host
  - A DHCP lease with associated objects and with a different MAC address than that of the discovered host
  - An Infoblox host address configured for DHCP services and with a different MAC address than that of the discovered host
- For a discovered host that is part of a DHCP range but does not have a fixed or leased address or is not within an exclusion range, the appliance assigns a DHCP range conflict to the IP address.
- For a discovered host through a vDiscovery, the appliance adds the discovered data to the database. The data is displayed in the IP Map and IP List panels, the Discovered Data tab of an object editor, and the Discovered Data section of the IP Address panel.
- The OS of an IP address obtained by an IP discovery supersedes that obtained by a vDiscovery, and the newly discovered name of a host supersedes the last discovered data.
- When a vDiscovery cannot obtain the IP address of a virtual entity, it does not return any discovered data for the entity.
- Only the objects with IP addresses to which the administrators have read/write permission are updated to include the vDiscovery data.
**Database Capacity**

When the Grid Master database reaches its maximum capacity (the maximum capacity varies based on the appliance model), the Grid Master stops updating the database and requests that the Grid member stop the discovery. When the discovering Grid member database reaches its capacity, the Grid member pauses the discovery. The appliance displays a dialog to inform you that the discovery pauses. The Grid member resumes the discovery once the database falls below its capacity. When a discovery pauses because of capacity issues, you cannot resume the discovery or start a new discovery. You can check the capacity of your appliance database before starting a discovery.

**HA Failover**

In an HA pair, if the Grid Master fails over to the passive node, the passive node takes over and continues with the discovery from the last known state. If an independent appliance fails, the appliance stops the discovery process and keeps the discovery in a paused state. The appliance resumes the discovery once it starts up again.

**Configuring IP Discovery**

You must have read/write permission to Network Discovery to initiate a discovery. After you start a discovery, you cannot change the configuration of the discovery, but you can start the discovery process immediately or schedule it for a later date. You can also configure a recurring discovery that repeats on a regular basis. For information, see Configuring and Starting an IP discovery and Scheduling IP Discovery. The appliance saves the configuration of the last discovery.

When you start an IP discovery from the IPAM Home, Net Map or Network List panel, you can select the networks on which you want the discovery to run. When you start an IP discovery from the IP Map or IP List panel, the discovered network is the one to which the IP addresses belong. You can include additional networks when you configure the IP discovery from the Discovery Manager wizard. You can run an IP discovery on multiple networks in one network view.

**Guidelines for Starting and Scheduling IP Discovery**

After you configure a discovery, you can start the discovery process immediately or schedule it for a later date. You can also configure a recurring discovery that repeats on a regular basis. When you start a discovery immediately or schedule for a later date after you configure it, the discovery happens only once and it will not be repeated. To repeat a discovery regularly, you can configure a recurring discovery. A recurring discovery occurs repeatedly based on the schedule you have configured. For more information about how to start a discovery immediately or schedule it for a later date, see Configuring and Starting an IP discovery and Scheduling IP Discovery.

You can configure IP discovery tasks independent of each other and each one contains a specific set of networks and discovery settings. Note the following guidelines about immediate, regular and recurring IP discovery tasks:

- You cannot run regular and recurring discovery processes concurrently.
- If a recurring discovery is scheduled to start when a discovery is in progress, the recurring discovery will be postponed to the next schedule time. The current recurring discovery will not be performed.
- You can pause and resume all discovery tasks.
- You cannot start a discovery when another one has been paused.
- You cannot use the start command to start a recurring discovery.
- Discovery permissions are applicable to all discovery tasks.
- When you start an IP discovery, only the available IP addresses in the network are discovered. The discovered data through a specific Discovery job can only be modified or deleted by the same Discovery job. When you start a different Discovery job to discover IP addresses in the same network and if some of the information in the network is changed, the newly discovered data and the originally discovered data (now old data) co-exist in the database. When you run the original Discovery job again, the old data is deleted or modified, or the new data is added depending on the information discovered.

**Configuring and Starting an IP discovery**

To start an IP discovery immediately after you configure it:

1. From the Data Management tab, select the IPAM tab, and then select Discovery -> Discover Now from the Toolbar.
2. In the Discovery Manager wizard, click the General tab, and then complete the following in the Basic tab:
   - **Current Status:** Displays the last discovery status and timestamp. This data is read-only.
   - **Member Name:** Click Select Member. In the Member Selector dialog box, select the Grid member from which you want to run the discovery. You can also use filters or the Go to function to find a specific member. For information, see Using Filters and Using the Go To Function.
   - **Merge the discovered data with existing data:** When you select this check box, the appliance merges the discovered data with the existing data. It appends newly discovered data to existing data and preserves the existing data when there is no newly discovered data. This check box is selected by default.

   **Note:** If you clear this check box, the appliance replaces the existing data with the newly discovered data and if there are no newly discovered values for some fields, the appliance removes the existing values for these fields and the fields become empty.

   - **Update discovered data for managed objects:** Select this check box if you want the appliance to update the data of existing managed objects such as A records, PTR records, host records, and fixed addresses, with the discovered data. If you clear this

Copyright ©2019, Infoblox, Inc. All right reserved.
check box, the appliance updates only the unmanaged objects. This check box is selected by default.

3. Click **Save** to save the discovery configuration. Note that you must save the configuration before you can start a discovery.

4. Click **Start** to start the IP discovery. You can also do one of the following:
   - **Restore to Defaults**: Restore the discovery configuration using the default values.
   - **Pause**: Stop a running discovery.
   - **Resume**: Resume the discovery that has been stopped.
   - **Save**: Save the discovery configuration.
   - **Close**: Cancel the configuration. If you have started a discovery, the discovery runs in the background when you click **Close**. For information, see **Running Tasks in the Background**.

**Note**: Once you start a discovery, you cannot change the discovery configuration. After you click **Start**, the button changes to **Pause**. You can click **Pause** to pause a discovery. When the discovery is paused, the button changes to **Resume**. You can click **Resume** to continue the paused discovery.

### Defining IP Discovery Method

To configure the IP discovery method you want to use:

1. From the **Data Management** tab, select the **IPAM** tab, and then select **Discovery -> Discover Now** from the Toolbar.

2. In the **Discovery Manager** wizard, click the **IPv4 Device Discovery** tab, and then complete the following in the **Basic** tab:
   - **Mode**: Select the IP discovery method you want to use. For information, see **Supported IP Discovery Methods**. If you select **TCP or FULL**, ensure that you configure the TCP ports in the **Advanced** tab. The default is **FULL**.
   - Click the Add icon to add networks. In the **Network Selector** dialog box, select the network view and networks. Use **SHIFT+click** and **CTRL+click** to select multiple networks. You can also use filters or the **Go** to function to find a specific network. For information, see **Using Filters** and **Using the Go To Function**.
     
     You can do the following in the table:
     - Click the Add icon again to add more networks.
     - Select a network or multiple networks in the network table and click **Delete** to delete them.
     - Click the Export icon to export the data in CSV format.
     - Click the Print icon to print the data.
   - **Disable**: Select this to exclude an IP discovery task. IP discovery is enabled by default.

3. If you select **TCP** or **FULL** in **Mode**, click the **Advanced** tab and complete the following:
   - **TCP Scan Technique**: Select the TCP technique you want to use for the discovery. The default is **SYN**. For information, see **TCP**.
   - In the port table, select the check box of the port you want to configure. You can select all ports by clicking the check box in the header. Optionally, you can click the Add icon and complete the following to add a new service to the list:
     - **Port**: Enter the port number you want to add to the list. You must enter a number between 1 and 65535.
     - **Service**: Enter the name of the service.
   - **Timeout (ms)**: Enter the timeout value in milliseconds for the discovery. The timeout value determines how long the discovery waits for a response from an IP address after probing it. The minimum is 5 and the maximum is 4000. The default is 1000.
   - **Attempts**: Enter the number of times you want the discovery to probe an IP address when scanning a network. The minimum is 1 and the maximum is 5. The default is 2.

4. Click **Save** to save the discovery configuration. Note that you must save the configuration before you can start a discovery.

5. Click **Start** to start the IP discovery. You can also do one of the following:
   - **Restore to Defaults**: Restore the discovery configuration using the default values.
   - **Pause**: Pause a running discovery.
   - **Resume**: Resume the discovery that has been stopped.
   - **Save**: Save the discovery configuration.
   - **Close**: Cancel the configuration. If you have started a discovery, the discovery runs in the background when you click **Close**. For information, see **Running Tasks in the Background**.

You can do the following after a discovery is complete:

- View the discovery status. You can view the current discovery status in the **Discovery Status** widget on the Dashboard. For information, see **Dashboards**.
- View the discovered data. For information, see **Viewing Discovered Data**.
- Manage the discovered data. For information, see **Managing Discovered Data**.

### Scheduling IP Discovery

After you configure a discovery (as described in **Configuring and Starting an IP discovery**), you can schedule to run a one-time IP discovery at a later date and time. You can also schedule a recurring IP discovery by configuring a recurrence pattern. The appliance automatically starts a recurring discovery based on the configured schedule and detects any newly added or removed networks. Note that you can only schedule the start of a discovery, you cannot schedule it to pause, stop, or resume. After a scheduled discovery starts, you can then pause, stop, or resume it. You can schedule only one IP discovery at a time. Once you schedule a discovery, you cannot change the configuration until the task is cancelled or executed. You can however disable a recurring discovery. When you disable a recurring discovery, it will not recur during the scheduled
interval.

To schedule a one-time IP discovery for a specific date and time:

1. From the Data Management tab, select the IPAM tab, and then select Discovery -> Discover Now from the Toolbar.
   or
   From the Discovery Status widget, select Discover Now from the drop-down list, and then click Discovery Manager.
2. In the Discovery Manager wizard, click the Schedule icon at the top of the wizard. In the Schedule Change panel, click Later, and then specify a date, time, and time zone. Click Schedule Start to schedule the discovery. If applicable, you can select Click here to view/manage the scheduled items to reschedule a discovery or view all scheduled discoveries.

To schedule a recurring IP discovery:

1. From the Data Management tab, select the IPAM tab, and then select Discovery -> Schedule Discovery from the Toolbar.
   or
   From the Discovery Status widget, select Schedule Discovery from the drop-down list, and then click Discovery Manager.
2. In the Discovery Manager wizard, complete the following in the scheduler:

   a. **Schedule every hour(s) at:** Enter the number of hours between each update instance. You can enter a value from 1 to 24.
      b. **Minutes past the hour:** Enter the number of minutes past the hour. For example, enter 5 if you want to schedule the rule update five minutes after the hour.
      c. **Time Zone:** Select the time zone for the scheduled time from the drop-down list.

   If you select Daily, you can select either Everyday or Every Weekday and then complete the following:

      a. **Time:** Enter a time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.
      b. **Time Zone:** Select the time zone for the scheduled time from the drop-down list.

   If you select Weekly, complete the following:

      a. **Schedule every week on:** Select any day of the week.
      b. **Time:** Enter a time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.
      c. **Time Zone:** Select the time zone for the scheduled time from the drop-down list.

   If you select Monthly, complete the following:

      a. **Schedule the day of the month:** Enter the day of the month and the monthly interval. For example, to schedule the rule update on the first day after every 2 months, you can enter Day 1 every 2 month(s).
      b. **Time:** Enter a time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.
      c. **Time Zone:** Select the time zone for the scheduled time from the drop-down list.

3. Click Save to save the configuration.

If the discovery task fails during a scheduled interval, the task stops and will not continue for the corresponding occurrence. The scheduled task resets and the discovery starts at the next scheduled time. For example, when you configure the recurring discovery to occur every five hours, discovery starts at the following hours on each day: 00:00, 05:00, 10:00, 15:00, and 20:00. If the discovery scheduled for 05:00 fails, the discovery starts at the next recurrence, which is at 10:00. For information about failed discovery, see Guidelines for Starting and Scheduling IP Discovery.

The following examples explain when a recurring discovery starts based on your configuration:

**Example 1**
When you configure a recurring discovery to occur every five hours, the discovery starts at the following hours on each day: 00:00, 05:00, 10:00, 15:00, and 20:00. The first occurrence on each day starts at 00:00.

**Example 2**
When you configure a recurring discovery to occur every two days during a week, the discovery starts on the following days every week: Monday, Wednesday, Friday, and Sunday. The first occurrence starts on Monday of each week.

### Monitoring IP Discovery Status

You can monitor IP discovery status through the Discovery Status widget on the Dashboard. You can also start, pause, resume, and stop a discovery from the widget. For information, see Discovery Status.

### Configuring vDiscovery Jobs

A vDiscovery job retrieves information about virtual entities in cloud environments that are managed through CMPs such as VMware, OpenStack, and AWS. You must first select a member to run the vDiscovery job. To ensure that the job is executed properly, verify the connection between the discovering member and the discovered endpoint. If you select HTTPS as the protocol for communication, you must upload either an SSL CA (Certified Authority) certificate or a self-signed SSL certificate to the Grid. For information about how to upload a certificate, see Managing Certificates.
After you upload a new certificate, wait for two minutes before running a vDiscovery job. This is because the newly uploaded certificate takes some time to be reflected in the NIOS database.

Note that when you disable any virtual entities or interfaces on the CMP, the appliance excludes them from the vDiscovery job. In situations where the discovering member you select to perform vDiscovery jobs is disconnected from the Grid Master, the member continues to execute vDiscovery jobs based on the configured schedule. Newly discovered data replaces previously discovered data. The last set of discovered data is considered the most up-to-date and is sent to the Grid Master when the member reconnects with the Grid Master.

When you configure vDiscovery jobs, you can enable the Infoblox NIOS appliance to automatically create DNS records for discovered IP addresses of VM instances that are served by the NIOS appliance. You can configure the appliance to add DNS records for specific DNS views associated with the network view defined for public and private IP addresses of VM instances served by the appliance. For more information about this feature, see Creating DNS Records for Newly Discovered VMs.

Before you configure and start a vDiscovery job, there are a few guidelines to consider. For more information, see Guidelines for Configuring vDiscovery Jobs.

Guidelines for Configuring vDiscovery Jobs
Consider the following guidelines before starting a vDiscovery job:

- Discovered data through a specific vDiscovery job can only be modified or deleted by the same vDiscovery job. If you create a different vDiscovery job to discover the same network and some of the information in the network has changed, the newly discovered data and the original discovered data (now old data) co-exist in the database. The old data is deleted only when you run the original discovery job again. For example, vDiscovery job “AWSJob1” discovers IP address 10.0.0.11 with VM name “corpxyz.” This discovered data is stored in the NIOS database. You subsequently create a new vDiscovery Job “AWSJob2” to discover the same IP but now the VM name has been changed to “corp200.” The discovered VM name for 10.0.0.11 is now “corp200.” Both VM names “corpxyz” and “corp200” exit in the database until you run AWSJob1 again, and “corpxyz” will be removed from the database.
- If the “ERROR: PycURL” error is displayed when you run a vDiscovery job, it is possible that the cloud provider has updated their certificate. You need to download the latest certificate from the cloud provider website and upload it to NIOS. For example, for AWS, download the certificates from [https://www.amazontrust.com/repository/](https://www.amazontrust.com/repository/). For information see Errpr while running job.
- Cloud Extensible Attributes:
  - To merge discovered cloud extensible attributes into NIOS, you must have at least one cloud license (Cloud Network Automation or Cloud Platform) installed in the Grid. However, if you want to view the discovered cloud data in the Cloud tab of Grid Manager, you must have the Cloud Network Automation license installed on the Grid Master. Otherwise, even though the cloud data is merged into the NIOS database, you cannot view it through Grid Manager. For information about Cloud Network Automation, see Deploying Cloud Network Automation.
  - In addition, ensure that you select the auto consolidation options when defining policies for how to handle the discovered cloud extensible attributes, as described in Defining Policies for Handling Discovered Data. Note that only cloud extensible attributes for managed objects are updated. To update cloud extensible attributes for unmanaged objects, you can first convert the unmanaged objects to managed objects. For more information, see Managing Unmanaged Data.

When you select VMware as the endpoint server for the vDiscovery job, consider the following:

- Typically, vDiscovery does not collect data about “Network” from VMware vSphere and vCenter servers. Therefore, you must first define a network in NIOS in order to discover IPs in the network.
- However, if you use vCenter to define a network as “IP_Pool,” which contains the CIDR for the network, vDiscovery is able to collect this data and translate it into a network. NIOS then creates the network and updates it with corresponding Cloud extensible attributes.

If you use an AWS Elastic IP address and select AWS as the endpoint server for the vDiscovery job, you must first manually create the network in NIOS before launching the vDiscovery job in order to discover the Elastic IP.

You cannot delete discovered tenants, networks, and VMs through the vDiscovery process. Conflict management is not supported for these objects. Note the following:

- Discovered subnets are always created as managed networks. Pools of IP addresses (public pools) when discovered are translated into managed networks. Any discovered public IP that is not linked to a pool is marked as unmanaged data in NIOS, unless there is a corresponding network already created.
- Tenant and VM information is merged into NIOS through cloud extensible attributes, only if there is a cloud license (Cloud Network Automation or Cloud Platform) installed in the Grid. Properties for unmanaged tenants and VMs are always updated while properties for managed tenants and VMs are updated only if auto-consolidation of tenant and VM information is selected when you configure the vDiscovery job. For information about auto-consolidation options, see Defining Policies for Handling Discovered Data.

- Properties of a VM address (such as interface name, network encapsulation, segmentation, VLAN ID) can only be updated through cloud extensible attributes, depending on the policies you select when configuring a vDiscovery task. To properly integrate discovered VM address properties with NIOS, ensure that you do one of the following:
  - Define cloud extensible attributes for these properties through your cloud adapter. For information about how to define cloud extensible attributes, refer to the Quick Start Guide for your cloud adapter, available on the Support site.
  - Convert unmanaged VM addresses to managed so discovered cloud extensible attributes can be merged into NIOS. For more information, see Converting Unmanaged Data.

- Unmanaged objects in NIOS are updated with newly discovered data and stay as unmanaged objects. Managed objects in NIOS that have no conflict with newly discovered data are updated and stay as managed objects.
- If there is conflict between managed objects in NIOS and newly discovered data, the managed objects are not updated and stay as managed objects while a conflict is flagged for these objects. For information about how to resolve the conflict, see Resolving Conflicting Addresses.
- NIOS does not automatically remove unmanaged objects that were discovered in the past but do not exist in current discoveries. This can happen if your network topology has changed in between discoveries. You can manually remove these unmanaged objects if you do not want them to stay in the database. For information about how to remove these objects, see Clearing Unmanaged Data.
For delegated DNS and DHCP objects, changes are handled by the delegated Cloud Platform Appliance based on the scope of delegation. Discovered data is still updated by the Grid Master.

To create a new vDiscovery job, complete the following tasks:

1. Name the new job and select a member to perform the vDiscovery, as described in Selecting the vDiscovery Member.
2. Select a cloud platform for the vDiscovery, as described in Selecting the Endpoint Server.
3. Define network views for public and private IP addresses, as described in Defining Network Views.
4. Define policies for handling discovered data, as described in Defining Policies for Handling Discovered Data.
5. Optionally, you can enable NIOS to automatically create DNS records for newly discovered VMs using their IP addresses, as described in Creating DNS Records for Newly Discovered VMs.
6. Schedule the vDiscovery job, as described in Scheduling vDiscovery Jobs.

Selecting the vDiscovery Member

To create a new or modify an existing vDiscovery job:

1. For a new vDiscovery job: From the Data Management tab, select the IPAM tab, then select vDiscovery -> New from the Toolbar; or from the Cloud tab, select vDiscovery -> New from the Toolbar.
   or
   To modify an existing job: From the Data Management tab, select the IPAM tab and click vDiscovery -> Discovery Manager from the Toolbar, or from the Cloud tab, select vDiscovery -> Discovery Manager from the Toolbar. In the vDiscovery Job Manager editor, click the Action icon (shown as a gear in each row) next to a selected job and select Edit from the menu.
2. In step one of the vDiscovery Job wizard or in the General tab of the vDiscovery Job Properties editor, complete the following:
   - **Job Name**: Enter the job name for this vDiscovery. It might be helpful to use a name that is unique to this specific discovery if you plan to configure multiple vDiscovery jobs.
   - **Member**: Click Select to choose the Grid member that will perform the vDiscovery job. If only a single member is active, the appliance name automatically appears here. When you select a Cloud Platform Appliance to perform vDiscovery, it communicates directly with the CMPs to obtain information that is not available through the provisioning process from the cloud adapter.
   - **Comment**: Enter information to describe this discovery. The new job will not execute until you have completed all configuration steps in the wizard. You will not be able to save this job until you have completed all job settings.
3. Click Next to select an endpoint server on which you want to perform the vDiscovery job, as described in Selecting the Endpoint Server, or save the configuration after you have modified data in this tab.

Selecting the Endpoint Server

1. For a new vDiscovery job: From the Data Management tab, select the IPAM tab, then select vDiscovery -> New from the Toolbar; or from the Cloud tab, select vDiscovery -> New from the Toolbar.
   or
   To modify an existing job: From the Data Management tab, select the IPAM tab and click vDiscovery -> Discovery Manager from the Toolbar, or from the Cloud tab, select vDiscovery -> Discovery Manager from the Toolbar. In the vDiscovery Job Manager editor, click the Action icon (shown as a gear in each row) next to a selected job and select Edit from the menu.
2. In step two of the vDiscovery Job wizard, or in the Endpoint tab of the vDiscovery Job Properties editor, complete the following:

   **Note**: You might lose some discovered data if you modify any of the following parameters for an existing vDiscovery job. To avoid this, create a new vDiscovery job instead.

   - **Server Type**: Choose one of the following server types for this vDiscovery:
     - **AWS**: Collects information available for the AWS service endpoint. You can perform vDiscovery jobs through a proxy server in an AWS deployment, including Amazon Route 53. For more information, see Configuring Proxy Servers.
     - **Azure**: Collects information available for virtual entities in the specified V Nets (Azure virtual networks) within the Microsoft Cloud.
     - **OpenStack**: When you select this server type, vDiscovery discovers network information stored in Neutron servers, VM instance information in Nova servers, and tenant or project information in Keystone servers.
     - **VMware**: Supports VMware vCenter and vSphere servers v5.0 and later. Collects information for all virtual entities running on the specified servers.

   Depending on the server type you select, other options in this step change accordingly, as follows:

   For AWS, complete the following:

   - **Service Endpoint**: This is typically the regional service endpoint for the desired Amazon region. Example: ec2.us-west-1.amazonaws.com. For more information about AWS service endpoints, refer to the Infoblox Installation Guide for vNICs for AWS, available on the Infoblox Support site.
   - **Port**: Enter the port you want to use for the vDiscovery job.
• **Protocol:** The protocol used for AWS is always over SSL. AWS provides certificates that is linked to the CA. By default, this certificate is embedded in NIOS and used as a reference for the CA when connecting to AWS. You can also upload a new certificate as described in *Managing Certificates.* If you upload a new certificate, the embedded certificate will be overwritten by the new one.

• **Allow unsecured connection:** This option is not applicable for AWS connection.

**Credentials:** Select the method you want to use to authenticate the connection between the Grid member and AWS for discovery jobs. You can select one of the following:

• **Use instance profile:** An instance profile is a container for an IAM role that you use to pass role information to an EC2 instance when the instance is up and running. Select this option if you want to collect information from AWS by waiving a user's credentials and using configuration of a predefined IAM role to get a temporary token that allows API calls. Note that you must first configure the option for “instance profile” in AWS, define an IAM role in the instance profile, and then set permissions for this role before you can select this option. Otherwise, this option is disabled. When you select this, you do not need to provide user credentials.

• **Use IAM credential:** Select this if you want to authenticate by using IAM roles to grant secure access to AWS resources from your EC2 instances. Click *Select* to choose the IAM role and use its credentials to access AWS resources from your EC2 instances when they are up and running.

  • **Access Key ID** and **Secret Access Key:** Enter the Access Key ID and Secret Access Key for the AWS service endpoint. This is the secret key pair for the administrator account that executes the discovery job. For more information, refer to the *Infoblox Installation Guide for vNIOS for AWS,* available on the Infoblox Support site.

For more information about instance profiles and IAM roles, refer to the AWS documentation.

For **Azure,** complete the following:

• **ServiceEndpoint:** This is the service endpoint for the desired VNet in the Microsoft Cloud. For more information about Azure service endpoints, refer to the *Infoblox Installation Guide for vNIOS for Azure.*

• **Port:** Enter the port you want to use for the vDiscovery job.

• **Protocol:** The protocol used for Azure is always over SSL. Azure provides certificates that is linked to the CA. By default, this certificate is embedded in NIOS and used as a reference for the CA when connecting to Azure. You can also upload a new certificate as described in *Managing Certificates.* If you upload a new certificate, the embedded certificate will be overwritten by the new one.

• **Allow unsecured connection:** This option is not applicable for Azure connection.

• **ClientID and ClientSecret:** Enter the client ID and client secret for the Microsoft Azure account. When you configure the client account, ensure that you have authorization to obtain device information on a wide network basis. For information about Azure client ID and client secret, refer to Microsoft Azure documentation.

**Note:** Azure Government Cloud uses different service endpoints for its services. For more information about Azure service endpoints, refer to the *Infoblox Installation Guide for vNIOS for Azure.*

For **OpenStack,** complete the following:

• **Keystone Server IP:** Enter the Keystone Server IP address.

• **Keystone Server Port:** Enter the Keystone Server Port value.

• **Protocol:** Select HTTP or HTTPS as the protocol. When you select HTTPS, you must upload the corresponding SSL CA certificate to the Grid in order for NIOS to communicate with OpenStack, as described in *Managing Certificates.*

• **Allow unsecured connection:** This option is enabled when you use HTTPS as the protocol. When you select this, the appliance bypasses remote SSL certificate validation. Select this option only if security for the HTTPS connection between the discovering member and OpenStack is irrelevant, or if the connection is protected by other security measure besides TSL/SSL, such as an isolated private circuit.

• **Username** and **Password:** Enter the username and password of the administrative account that was configured on OpenStack. When you configure the administrative account, ensure that you have authorization to obtain device information on a wide network basis.

• **Identity Version:** Select the Keystone server identity service version from the drop-down list. You can select one of the following: **Keystone v2** and **Keystone v3.** By default, **Keystone v2** is selected.

• **Domain Name:** Enter the domain name. This field is displayed only if you select **Keystone v3** as the identity version.

For **VMware,** complete the following:

• **Host:** Enter the host name of the VMware server.

• **Port:** Enter the port number of the VMware server.

• **Protocol:** Select HTTP or HTTPS as the protocol. When you select HTTPS, you must upload the corresponding SSL CA certificate in order for NIOS to communicate with the VMware server, as described in *Managing Certificates.*

• **Allow unsecured connection:** This option is enabled when you use HTTPS as the protocol. When you select this, the appliance bypasses remote SSL certificate validation. Select this option only if security for the HTTPS connection between the discovering member and VMware server is irrelevant, or if the connection is protected by other security measure besides TSL/SSL, such as an isolated private circuit.

• **Username** and **Password:** Enter the username and password of the administrative account that was configured on the specified VMware server. When you configure the administrative account, ensure that you have authorization to obtain device information.

Click **Next** to define the network views to which discovered data belongs for both public and private IP addresses, as described in *Defining Network Views.*
To track overlapping networks and IP address ranges so you can discover specific networks and IP addresses, you can associate one or more network views with a Grid member or Cloud Platform Appliance that is selected to run the vDiscovery. You can then define a specific network view to which discovered data for public and private IP addresses belongs if the network view is not automatically detected. If no network view is specified, the default network view is used.

For Network Insight, when you discover networks using multiple discovery interfaces, you must configure network views so you can associate each discovery interface with an available network view. Note that on the same discovering member, each discovery interface must have a unique network view association.

1. **For a new vDiscovery job:** From the **Data Management** tab, select the **IPAM** tab, then select **vDiscovery -> New** from the Toolbar; or from the **Cloud** tab, select **vDiscovery -> New** from the Toolbar.
   
   or
   
   To modify an existing job: From the **Data Management** tab, select the **IPAM** tab and click **vDiscovery -> Discovery Manager** from the Toolbar, or from the **Cloud** tab, select **vDiscovery -> Discovery Manager** from the Toolbar. In the **vDiscovery Job Manager** editor, click the Action icon
   
   (shown as a gear in each row) next to a selected job and select **Edit** from the menu.

2. In step three of the **vDiscovery Job** wizard, or in the **Network View** tab of the **vDiscovery Job Properties** editor, complete the following:
   
   - Under the **For Public IP Addresses** section, select one of the following options the appliance uses if the network view is not automatically detected:
     
     - **This Network View**: From the drop-down list, specify a network view to which discovered data for public IP addresses belongs. The default is the default network view. You cannot create a new network view for this option.
     
     - **The tenant's network view (if it does not exist, create a new one)**: Select this only if at least one cloud license is installed in the Grid. When you select this, discovered data for public IP addresses belongs to the tenant's network view. If the network view does not exist, the appliance creates it (only if a cloud license is installed in the Grid). The appliance uses tenant information of a discovered public IP address to create a new NIOS network view for all discovered objects (primarily subnets) for that tenant. For example, AWS tenants by default are associated with the user account's 12-digit account number (such as 2233441247523), which is the identifier for all objects that are created by that account in AWS. That tenant value becomes the identifier for the new network view as its objects are discovered by NIOS.
     
   - Under the **For Private IP Addresses** section, select one of the following options the appliance uses if the network view is not automatically detected:
     
     - **This Network View**: From the drop-down list, select a network view to specify a network view to which discovered data for private IP addresses belongs. The default is the default network view. You cannot create a new network view for this option.
     
     - **The tenant's network view (if it does not exist, create a new one)**: Select this only if at least one Cloud Platform Appliance is active or a cloud license is installed in the Grid. When you select this, discovered data for private IP addresses belongs to the tenant's network view. If the network view does not exist, the appliance creates it (only if a cloud license is installed in the Grid). The appliance uses tenant information of a discovered private IP address to create a new NIOS network view for all discovered objects (primarily subnets) for that tenant. For example, AWS tenants by default are associated with the user account's 12-digit account number (such as 2233441247523), which is the identifier for all objects that are created by that account in AWS. That tenant value becomes the identifier for the new network view as its objects are discovered by NIOS.

3. Click **Next** to configure how you want the appliance to handle discovered data, as described in **Defining Policies for Handling Discovered Data**.

**Defining Policies for Handling Discovered Data**

In this step, you define how the appliance handles discovered data.

1. **For a new vDiscovery job:** From the **Data Management** tab, select the **IPAM** tab, then select **vDiscovery -> New** from the Toolbar; or from the **Cloud** tab, select **vDiscovery -> New** from the Toolbar.
   
   or
   
   To modify an existing job: From the **Data Management** tab, select the **IPAM** tab and click **vDiscovery -> Discovery Manager** from the Toolbar, or from the **Cloud** tab, select **vDiscovery -> Discovery Manager** from the Toolbar. In the **vDiscovery Job Manager** editor, click the Action icon
   
   (shown as a gear in each row) next to a selected job and select **Edit** from the menu.

2. In step four of the **vDiscovery Job** wizard, or in the **Data Consolidation** tab of the **vDiscovery Job Properties** editor, complete the following:

   Under **When inserting discovered into NIOS**, select one or both of the following:

   - **Merge the discovered data with existing data**: When you select this check box, the appliance merges the discovered data with the existing data. It appends newly discovered data to existing data and preserves the existing data when there is no newly discovered data. This check box is selected by default.

   **Note**: If you clear this check box, the appliance replaces the existing data with the newly discovered data and if there are no newly discovered values for some fields, the appliance removes the existing values for these fields and the fields become empty.

   - **Updated discovered data from managed objects**: Select this check box if you want the appliance to update discovered data for all
corresponding NIOS objects (if they exist in NIOS). If you do not select this check box, the appliance updates only the discovered data for unmanaged objects. None of the managed data will be updated. This check box is selected by default.

- **ForeverynewlydiscoveredIPAddress, create**: Select this check box to enable NIOS to automatically create or update DNS records for discovered network entities and VM instances (except for cloud adapters such as AWS or DDNS) if the records were originally created by vDiscovery. For more information about this feature, see Creating DNS Records for Newly Discovered VMs.

- **Host**: Select this to automatically create Host records for discovered entities.

- **A&PTRRecord**: Select this to automatically create A and PTR records for discovered entities. Note that the DNS zones and reverse-mapping zones to which the records belong must exist in NIOS before the vDiscovery job is executed. Otherwise, vDiscovery does not create the records.

- **TheDNSNamewillbecomputedfromtheformula**: Enter the formula that NIOS uses to create the DNS records for each discovered network address. For example, if there are two IP addresses associated with a VM, NIOS creates two DNS records, or a host record with two IP addresses, depending on your configuration. You must use the syntax of \$\{parameter name\} for the formula.

For AWS, OpenStack, and VMware cloud platforms, this field supports the following parameters: \$\{vm_id\}, \$\{vm_name\}, \$\{discover_name\}, \$\{tenant_ID\}, \$\{tenant_name\}, \$\{vport_name\}, \$\{ip_address\}, \$\{ip_address_octet1\} or \$\{ip_address_octet2\} or \$\{ip_address_octet3\} or \$\{ip_address_octet4\} or 4. Note that it does not support IPv6 addresses.

For example, when you enter \$\{vm_name\}.corpxyz.com and the discovered \$\{vm_name\} = XYZ, the DNS name for this IP becomes XYZ.corpxyz.com. When you enter \$\{discover_name\} here and the discovered name for the IP is ip-172-31-1-64.us-west-1.compute.internal, the DNS name for this IP is ip-172-31-1-64.us-west-1.compute.internal.

- Under **Select the DNS view to which the DNS records are being added**, select one or both of the following:

  - **Use this DNS view for public IPs**: Select this check box to add DNS records to a specific DNS view for public IPs. Select a DNS view from the drop-down list. If you do not select a DNS view, the DNS records are added to the default DNS view.

  - **Use this DNS view for private IPs**: Select this check box to add DNS records to a specific DNS view for private IPs. Select a DNS view from the drop-down list. If you do not select a DNS view, the DNS records are added to the default DNS view.

Note that the **Use this DNS view for public IPs** and **Use this DNS view for private IPs** fields will be disabled, if you select The tenant’s network view (if it does not exist, create a new one) option when you define the network views to which discovered data belongs for both public and private IP addresses, as described in Defining Network Views.

Under **When discovered data is linked to managed data**, select any combination of the following.

**Note**: Tenants and VMs are managed objects when they have Host records or fixed addresses, associate with them. Otherwise, they are unmanaged objects. The appliance always updates properties for all unmanaged objects.

- **Auto-consolidate on managed Tenant’s properties**: When you select this check box, the appliance updates properties with discovered data for managed tenants, as well as unmanaged tenants (NIOS always update unmanaged tenants). When you clear this check box, the appliance does not update discovered data for managed tenants. This check box is selected by default.

- **Auto-consolidate managed VM’s properties**: When you select this check box, the appliance updates properties with discovered data for managed VMs, as well as unmanaged tenants (NIOS always update unmanaged tenants). When you clear this check box, the appliance does not update discovered data for managed VMs. This check box is selected by default.

- **Auto-consolidate Cloud EAs on managed data**: When you select this check box, NIOS updates discovered extensible attribute values for managed objects that contain cloud extensible attributes, only if a cloud license is installed in the Grid. This includes the update of the extensible attribute VM ID (which links the NIOS object to the VM) whenever a VM is added, updated or removed depending on the information collected. As a result, when a VM instance reuses an IP address or when a VM instance is deleted in the Cloud, the DNS Records or fixed address tied to that IP address are also updated, reflecting the new value of the VM instance ID. To update cloud extensible attributes for unmanaged objects, convert the objects to managed objects in NIOS. For more information, see Managing Unmanaged Data.

**Note**: The extensible attribute VM ID is not updated if you do not enable the Auto-consolidate Cloud EAs on managed data check box, which leads to a conflict on that IP address. The NIOS object does not link to the same VM as the newly discovered IP. In such cases, you can use the Resolve Conflicts option to update either your NIOS objects or your discovered data. For information about resolving conflicts, see Resolving Conflicting Addresses.

3. Click **Next** to schedule this vDiscovery job and specify when the job should start, as described in Scheduling vDiscovery Jobs.

Creating DNS Records for Newly Discovered VMs

When you configure the policies NIOS uses to handle discovered data, you can enable NIOS to automatically create or update DNS records for discovered IP addresses of VM instances. NIOS automatically adds Host records or A and PTR records for the discovered VMs based on your configuration. You can also enter a formula that NIOS uses to create the DNS name for the discovered IP based on its VM parameters such as VM name or discovered name. By doing so, NIOS is able to discover public and private IP addresses by looking up the corresponding DNS names.

Discovered data includes IP addresses for the VMs and the associated information such as VM ID, VM Name, Tenant ID, and others. Note that corresponding zones must already exist in order for NIOS to add DNS records. Otherwise, NIOS does not add any DNS records and it logs a message in the syslog. For information about how to enable this feature, see Defining Policies for Handling Discovered Data.

NIOS automatically adds DNS records based on the following conditions:

Copyright ©2019, Infoblox, Inc. All right reserved.
The corresponding DNS zones must already exist in the NIOS database. NIOS does not automatically create DNS zones for the records.

- To create a PTR record, the corresponding reverse-mapping zone must exist.
- A DNS zone cannot be associated with more than one DNS view. NIOS does not create DNS records for zones that are associated with multiple DNS views.
- NIOS adds new DNS records only if the VM name for the discovered IP address is available and there is no conflict with information about the associated network view.

On subsequent vDiscovery, if an IP for a VM is removed, the corresponding DNS records are removed. If the IP for a VM is changed, the IP address in the corresponding DNS record is changed accordingly. If the DNS record name template is changed, all the DNS records are replaced with the DNS records using the new template. All administrative actions for these changes are recorded in the Audit log. Summary of the changes are logged in the syslog.

The following table captures some scenarios about how vDiscovery handles various actions and what the outcome is for the information on the Cloud Platform appliance and in the NIOS database. All the scenarios in the table use the following template: $(discovered_name).

**Note:** vDiscovery updates only records that are created by the vDiscovery process. It does not create or update DNS records that are originally created by other admin users.

<table>
<thead>
<tr>
<th>Actions and Conditions</th>
<th>Cloud Platform Data before vDiscovery</th>
<th>Cloud Platform Data after vDiscovery</th>
<th>NIOS Data before vDiscovery</th>
<th>NIOS Data after vDiscovery</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add new VM (vma) on Cloud Platform appliance</strong></td>
<td>No data for vma</td>
<td>10.10.10.1 vma.corp1.com</td>
<td>Zone: corp1.com</td>
<td>Zone: corp1.com Host record: vma.corp1.com (10.10.10.1)</td>
</tr>
<tr>
<td><strong>Automatic creation of Host records</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>In NIOS:</strong> existing zone corp1.com; no DNS records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **Add new VM (vma) on Cloud Platform appliance** | No data for vma | 10.10.10.1 vma.corp1.com | Zone: corp1.com Host record: vma.corp1.com (10.10.10.1) | Zone: corp1.com Host record: vma.corp1.com (10.10.10.1) |
|• Add new interface to existing VM (vma) with the same discovered name on Cloud Platform appliance | 10.10.10.1 vma.corp1.com | 10.10.10.1 vma.corp1.com | Zone: corp1.com Host record: vma.corp1.com (10.10.10.1) |
|• Automatic creation of Host records | 10.10.1 vma.corp1.com | 10.10.10.2 vma.corp1.com | Zone: corp1.com Host record: vma.corp1.com (10.10.10.1) |

**In NIOS:**
- existing zone corp1.com;
- existing Host record (originally created by vDiscovery)

<p>|• Add new interface to existing VM (vma) with the same discovered name on Cloud Platform appliance | 10.10.10.1 vma.corp1.com | 10.10.10.1 vma.corp1.com | Zone: corp1.com Host record: vma.corp1.com (10.10.10.1, 10.10.10.2) |
|• Automatic creation of Host records | 10.10.10.2 vma.corp1.com | 10.10.10.2 vma.corp1.com | Zone: corp1.com Host record: vma.corp1.com (10.10.10.1) |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Add a new interface to existing VM (vma) with a different discovered name (vma-if2) on the Cloud Platform appliance.</td>
</tr>
<tr>
<td>2.</td>
<td>Automatic creation of Host records.</td>
</tr>
<tr>
<td>3.</td>
<td>In NIOS: existing zone corp1.com; existing Host record (originally created by vDiscovery)</td>
</tr>
</tbody>
</table>

**existing zone corp1.com**

<table>
<thead>
<tr>
<th>Zone:</th>
<th>corp1.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host record:</td>
<td>vma.corp1.com (10.10.10.1)</td>
</tr>
<tr>
<td>Host record:</td>
<td>vma-if2.corp1.com (10.10.10.2)</td>
</tr>
</tbody>
</table>

**existing Host record (originally created by vDiscovery)**

<table>
<thead>
<tr>
<th>Zone:</th>
<th>corp1.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host record:</td>
<td>vma.corp1.com (10.10.10.1)</td>
</tr>
<tr>
<td>Host record:</td>
<td>vma-if2.corp1.com (10.10.10.2)</td>
</tr>
<tr>
<td>Action</td>
<td>Zone:</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Remove existing VM (vma) on Cloud Platform appliance</td>
<td>corp1.com</td>
</tr>
<tr>
<td>Automatic creation of Host records</td>
<td></td>
</tr>
<tr>
<td>In NIOS: existing zone corp1.com; existing Host record (originally created by v Discovery)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Zone:</th>
<th>Host record:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove existing VM (vma) with different discovered name (vma-if2) on Cloud Platform appliance</td>
<td>corp1.com</td>
<td>vma-if2.corp1.com (10.10.10.2)</td>
</tr>
<tr>
<td>Automatic creation of Host records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In NIOS: existing zone corp1.com; existing Host record (originally created by v Discovery)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- Remove existing interface (10.10.10.2) from VM (vma) with different discovered name (vma-if2) on Cloud Platform appliance
- Automatic creation of Host records
- In NIOS: existing zone corp1.com; existing Host record (originally created by a admin)

<table>
<thead>
<tr>
<th>Zone: corp1.com</th>
<th>Host record: vma.corp1.com (10.10.10.1)</th>
<th>Host record: vma-if2.corp1.com (10.10.10.2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>vma.corp1.com</td>
<td>vma-if2.corp1.com</td>
</tr>
<tr>
<td>10.10.10.1</td>
<td>vma.corp1.com</td>
<td>vma-if2.corp1.com</td>
</tr>
</tbody>
</table>

- Update record name (from vma to vm1) for the existing interface (10.10.10.1) on Cloud Platform appliance
- Automatic creation of Host records
- In NIOS: existing zone corp1.com; existing Host record (originally created by a Discovery)

<table>
<thead>
<tr>
<th>Zone: corp1.com</th>
<th>Host record: vma.corp1.com (10.10.10.1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>vma.corp1.com</td>
</tr>
<tr>
<td>10.10.10.1</td>
<td>vma.corp1.com</td>
</tr>
</tbody>
</table>

Copyright ©2019, Infoblox, Inc. All right reserved.
<table>
<thead>
<tr>
<th>Update record name (from vma to vm1) for the existing interface (10.10.10.1) on Cloud Platform appliance</th>
<th>10.10.10.1 vma.corp1.com</th>
<th>10.10.10.1 vm1.corp1.com</th>
<th>Zone: corp1.com Host record: vma.corp1.com (10.10.10.1)</th>
<th>Zone: corp1.com Host record: vm1.corp1.com (10.10.10.1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic creation of Host records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In NIOS: existing zone corp1.com; existing Host record (originally created by admin)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.10.10.1 vma.corp1.com</td>
<td>10.10.10.1 vm1.corp1.com</td>
<td>Zone: corp1.com Host record: vma.corp1.com</td>
<td>Zone: corp1.com Host record: vm1.corp1.com</td>
</tr>
<tr>
<td>Automatic creation of Host records</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change FQDN template from $(discover_name) to</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$(vm_name).corp1.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In NIOS: existing zone corp1.com; existing Host record (originally created by vDiscovery)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Automatic creation of Host records
- Change FQDN template from `${discover_name}` to `${vm_name}.corp1.com`

#### In NIOS:
- existing zone corp1.com
- existing Host record (originally created by a admin)

### Change vDiscovery task configuration from creation of Host record to A and PTR records
- In NIOS:
  - existing zone corp1.com
  - existing Host record (originally created by vDiscovery)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1 vm.corp1.com</td>
<td>10.10.10.1 vm.corp1.com</td>
<td>10.10.10.1 vm.corp1.com</td>
</tr>
<tr>
<td>Host record: vm.corp1.com (10.10.10.1)</td>
<td>Host record: ABC.corp1.com (10.10.10.1)</td>
<td>Host record: ABC.corp1.com (10.10.10.1)</td>
</tr>
</tbody>
</table>

### Scheduling vDiscovery Jobs

You can enable the appliance to start a vDiscovery immediately after you configure it, schedule it for a later date and time, or configure a recurring...
discovery based on a recurrence pattern. Note that all scheduled vDiscovery jobs are executed in queue based on the order of the schedule in the vDiscovery Job Manager. Therefore, a scheduled vDiscovery might be delayed if there are other jobs being executed before its scheduled start time.

1. For a new vDiscovery job: From the Data Management tab, select the IPAM tab, then select vDiscovery -> New from the Toolbar; or from the Cloud tab, select vDiscovery -> New from the Toolbar.
   or
   To modify an existing job: From the Data Management tab, select the IPAM tab and click vDiscovery -> Discovery Manager from the Toolbar, or from the Cloud tab, select vDiscovery -> Discovery Manager from the Toolbar. In the vDiscovery Job Manager editor, click the Action icon
   (shown as a gear in each row) next to a selected job and select Edit from the menu.
2. In step five of the vDiscovery Job wizard, or in the Schedule tab of the vDiscovery Job Properties editor, complete the following:
   - Enable: To ensure that the scheduled vDiscovery job takes place, select this check box. When you upgrade from a previous version of NIOS, you must select this check box after the upgrade to ensure that the previously configured discovery tasks are being executed at the scheduled time.

If you select Once, complete the following:
   - Choose a Start Date using the date picker.
   - Time Zone: Select the time zone for the scheduled time from the drop-down list.

If you select Hourly, complete the following:
   - Schedule every hour(s) at: Enter the number of hours between each update instance. You can enter a value from 1 to 24.
   - Minutes past the hour: Enter the number of minutes past the hour. For example, enter 5 if you want to schedule the rule update five minutes after the hour.
   - Time Zone: Select the time zone for the scheduled time from the drop-down list.

If you select Daily, you can select either Every day or Every Weekday and then complete the following:
   - Time: Enter a time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.
   - Schedule every hour(s) on: Select any day of the week.
   - Schedule every day on: Select any day of the week.
   - Time Zone: Select the time zone for the scheduled time from the drop-down list.

3. Save the vDiscovery job. The appliance lists all vDiscovery jobs in the vDiscovery Job Manager, from which you can manage jobs that have not been executed, including modifying selected jobs or deleting some. For more information about how to manage vDiscovery jobs, see Managing vDiscovery Jobs.

Managing vDiscovery Jobs

You can view all configured vDiscovery jobs or modify some of the settings for selected ones in the vDiscovery Job Manager. You can also add a new vDiscovery job by clicking the Add icon.

To view or modify vDiscovery jobs:

1. From the Data Management tab, select the IPAM tab, then select vDiscovery -> Discovery Manager from the Toolbar; or from the Cloud tab, select vDiscovery -> Discovery Manager from the Toolbar.
2. The appliance displays the following information in the vDiscovery Job Manager:
   - Name: The name of the vDiscovery job.
   - Status: The current status of the vDiscovery job. Grid Manager displays an icon and descriptive information about the status.
     You can hover mouse over the icon to view the current status, as follows:
     - Job created: The configured job has been created.
     - Job starting: Starting the configured job.
     - Job in progress: The job is being executed at the moment.
     - Job completed: The job is completed successfully.
     - Cancelled: The job was cancelled while it was being executed.
     - Error while running job: The job has failed.
     If the “ERROR: PycURL error: (60, “SSL certificate problem: unable to get local issuer certificate”)” error message is displayed, it means that the certificate has expired or is invalid. You need to remove the expired or invalid certificate and upload a new one. If the error is displayed for an AWS vDiscovery job, download the certificates from https://www.amazonaws/ontrust.com/repository/ and upload them. If it is displayed for an Azure vDiscovery job, follow the instructions in the
Viewing Discovered Data

After an IP discovery and a vDiscovery, you can view discovered data in the Discovered Data section when you drill down to a specific IP address in the Net Map, Net List, IP Map or IP List panel. For information about IP Map and IP List, see IP Map and IP Address List.

You can also view discovered data for Cloud specific VMs in the Cloud tab. Note that you must install the Cloud Network Automation license on the Grid Master to view the Cloud tab.

Viewing IPAM Discovered Data

To view discovered data in the IPAM tab:

1. In the top navigation bar, select the network view to which discovered data belongs.
2. From the Data Management tab, select the IPAM tab.
3. In the IPAM home page, select the network you want to view discovered data and click the link.
4. In the IP List of IP Map panel, click the IP address link to drill down to the IP address properties panel.
5. In the Discovered Data section, click the Configure icon to specify data to be displayed in the Discovered Data tab.
6. Select fields from the Available list and click the arrow key to move them to the Selected list and vice versa. You can use CTRL+Click or SHIFT+Click to select multiple fields at one time.
   You can also change the order in which the fields are displayed by moving the fields up and down in the Selected list. To move a field up in the list, select it and click the Up arrow. To move a field down, select it and click the Down arrow.
7. Click the Configure icon again, and the Discovered Data section displays the fields you have specified. Note the fields you select appears for all IP addresses in the network.

Depending on the source of the discovered data, when you modify certain DNS and DHCP objects, Grid Manager can display some of the following discovered data (if any) in the Discovered Data tab:

- **NetBIOSName**: The name returned in the NetBIOS reply or the name you manually register for the discovered host.
- **OS**: The operating system of the detected host or virtual entity. The OS can be one of the following:
  - **Microsoft**: For all discovered hosts that have a non-null value in the MAC addresses using the NetBIOS discovery method.
  - **A value that is a TCP discovery returns**.
  - **The OS of a virtual entity on a vSphere server**.
- **Discoverer MAC Address**: The discovered MAC address for the host. This is the unique identifier of a network device. The discovery acquires the MAC address for all hosts that are located on the same network as the Grid member that is running the discovery. This can also be the MAC address of a virtual entity on a specified vSphere server.
- **AP Name**: The name of the access point for the device. This column is displayed only for wireless devices.
- **AP IP Address**: The IP address of the access point for the device. This column is displayed only for wireless devices.
- **SSID**: The unique name of the WLAN (Wireless Local Area Network).
- **Discoverer DUID**: For IPv6 address only. The DHCP unique identifier of the discovered host. This is an optional field, and data might not be included.
- **Last Discovered**: The timestamp when the IP address was last discovered.
- **First Discovered**: The timestamp when the IP address was first discovered.
- **Task Name**: The name of the task that collected the discovered data. It is usually the ID or task name that collected the data. It is defined on the corresponding NetMRI appliance when you import the discovered data to the NIOS appliance. The task name should be defined in the vDiscovery task manager for vDiscovery.
- **Discoverer Name**: The name of the network device associated with the discovered IP address.
- **Discoverer**: Specifies whether the IP address was discovered by NetMRI or NIOS discovery process.
If you imported data from NetMRI appliances, Grid Manager displays the following information, if available. For information about the data imported from NetMRI appliances, see Integrating Discovered Data From NetMRI.

- **Attached Device Description**: A textual description of the switch that is connected to the end device.
- **Attached Device Address**: The IPv4 or IPv6 address of the switch that is connected to the end device.
- **Attached Device Model**: If a reverse lookup was successful for the IP address associated with this switch, the device model is displayed here.
- **Attached Device Name**: If a reverse lookup was successful for the IP address associated with this switch, the host name is displayed here.
- **Attached Device Port Description**: A textual description of the switch port that is connected to the end device.
- **Attached Device Port Name**: The name of the switch port connected to the end device.
- **Attached Device Port**: The number of the switch port connected to the end device.
- **Attached Device Type**: Identifies the switch that is connected to the end device.
- **Attached Device Location**: The physical location of the network device to which the end host is connected/attached, as detected from the device during discovery.
- **Attached Device Contact**: The contact details for the network device to which the End Host is connected/attached, as detected from the device during discovery.
- **Device Vendor**: The vendor name of the end device.
- **Device Model**: The device model of the end device.
- **Device Location**: The physical location of the network device on which the IP Address is configured, as detected from the device during discovery.
- **Device Contact**: The contact details for the network device on which the IP Address is configured, as detected from the device during discovery.
- **Device Management IP**: The IPv4 or IPv6 address of the end device that is connected to the switch.
- **Device Port Type**: The port type for the end device.
- **Device Port Name**: The port name for the end device.
- **Device Type(s)**: Identifies the device type.
- **Port Duplex**: The negotiated or operational duplex setting of the switch port connected to the end device. You can modify this in the IPv6 fixed address and AAAA record editors.
- **Port Link**: The link status of the switch port connected to the end device. Indicates whether it is connected.
- **Port Speed**: The interface speed, in Mbps, of the switch port. You can modify this in the IPv6 fixed address and AAAA record editors.
- **Port Type**: The switch port type.
- **Port Status**: The operational status of the switch port. Indicates whether the port is up or down.
- **Open Port(s)**: Ports that are open.
- **VLAN Description**: The description of the VLAN of the switch port that is connected to the end device.
- **VLAN Name**: The name of the VLAN of the switch port.
- **VLAN ID**: The ID of the VLAN of the switch port.

For IP addresses discovered through a vDiscovery, Grid Manager displays the following additional information, if available:

- **Virtual Host Adapter**: The name of the physical network adapter through which the virtual entity is connected to the appliance.
- **Virtual Datacenter**: The name of the vSphere datacenter or container to which the virtual entity belongs.
- **Virtual Cluster**: The name of the VMware cluster to which the virtual entity belongs.
- **Virtual Entity Name**: The name of the virtual entity.
- **Virtual Entity Type**: The virtual entity type. This can be blank or one of the following: Virtual Machine, Virtual Host, or Virtual Center. Virtual Center represents a VMware vCenter server.
- **Virtual Host**: The name of the VMware server on which the virtual entity was discovered.
- **Virtual Switch**: The name of the switch to which the virtual entity is connected.
- **Virtual Machine Name**: The name of the VM instance.
- **Virtual Machine ID**: The ID of the VM.
- **Virtual Machine Tenant ID**: The tenant ID to which the VM belongs.
- **Virtual Machine Port Group**: The port group to which the VM belongs.
- **Attached Virtual Switch Name**: The name of the virtual switch to which the VM is connected.
- **Attached Virtual Switch ID**: The ID of the virtual switch to which the VM is connected.
- **Attached Virtual Switch Type**: The type of the virtual switch. This can be standard or distributed.
- **Attached Virtual Switch IPv6 Enabled**: Indicates that virtual switch that has IPv6 enabled.
- **Attached Virtual Port Name**: The name of the virtual adapter on the virtual switch to which the VM is connected.
- **Attached Virtual Port MAC Address**: The MAC address of the virtual adapter on the virtual switch to which the VM is connected.
- **Attached Virtual Port Link Status**: The link status of the virtual adapter on the virtual switch to which the VM is connected.
- **Attached Virtual Port Configured Speed**: The configured port speed of the virtual adapter on the virtual switch to which the VM is connected.
- **Attached Virtual Port Configured Mode**: The configured mode of the virtual adapter on the virtual switch to which the VM is connected.
- **Attached Virtual Port Configured Speed**: The actual port speed of the virtual adapter on the virtual switch to which the VM is connected.
- **Attached Virtual Port Configured Mode**: The actual mode of the virtual adapter on the virtual switch to which the VM is connected.
- **Network Segment Type**: The type of network segment to which the VM is connected.
- **Network Segment Name**: The name of the network segment to which the VM is connected.
- **Network Segment ID**: The ID of the network segment to which the VM is connected.
- **Network Segment Port Group**: The port group of the network segment to which the VM is connected.
- **Network Segment Available Ports**: The number of available ports reported by the virtual switch to which the VM is connected.
Viewing Discovered Data for Cloud VMs

You can view discovered data for cloud specific VMs after performing a vDiscovery job. Note that you must have at least read-only permission to “All Tenants” and “All Network Views” to view the VMs tab.

To view discovered data for cloud VMs, see Viewing All Cloud VMs.

Managing Discovery Data

In addition to viewing the discovered data, you can do the following to manage the discovered data:

- Manage an unmanaged address by adding it to a host, converting it to managed data, or clearing its unmanaged status. Note that for Cloud Network Automation, you can convert discovered data to NIOS objects within a delegated scope. For information, see Managing Unmanaged Data.
- Resolve conflicting addresses. For information, see Resolving Conflicting Addresses.
- Clear discovered data for a network view, network, IP address, or cloud tenant. For information, see Clearing Discovered Data.
- You can also clear all discovered data collected by a specified vDiscovery job. For information see Clearing All Discovery Data.

Managing Unmanaged Data

You can manage unused and unmanaged addresses by doing one of the following:

- Add to an existing host, as described in Adding to an Existing Host.
- Convert to a fixed address, host, A record, or PTR record, as described in Converting Unmanaged Data. Note that for Cloud Network Automation, you can convert discovered data to NIOS objects within a delegated scope.
- Clear the unmanaged status, as described in Clearing Unmanaged Data.

Note: You cannot convert unmanaged IP addresses served by Microsoft DHCP servers to host records.

Adding to an Existing Host

You can add an unmanaged address, including all its information, to an existing host. You can select the desired host to which you want to add the unmanaged address.

To add an unmanaged address to an existing host:

1. From the IP Map or List panel, select an unmanaged address you want to add to a host, and then click Add -> Add to Existing Host from the Toolbar.
2. In the Select Host dialog box, select a host from the table. You can also search for a host using filters or the Go to function. For information, see Using Filters and Using the Go To Function. Click the Select icon to select the desired host.

Note: Depending on the page size configuration, the search results are limited to the page size that you set. If the search results exceed the page size limit, the appliance displays an error message to inform you to refine your search criteria or to change the page size limit. In the Host Record editor, complete the information as described in Choose one of the following from the Save & ... drop-down button menu.

3. Save the configuration and click Restart if it appears at the top of the screen.

Converting Unmanaged Data

You can convert an unmanaged address to a host, an A or AAAA record, a PTR record, or a fixed address. To convert an unmanaged address:

1. In the IP Map or List panel, select an unmanaged address you want to convert, and then select Convert from the Toolbar.
2. In the drop-down list, select the type of address to which you want to convert the unmanaged address. For IPv4 addresses, you can select To Host, To A Record, To PTR Record, or To Fixed Address. For IPv6 addresses, you can select To Host, To AAAA, To PTR.
Record, or To IPv6 Fixed Address.
Depending on the record type you select, Grid Manager displays the corresponding editor. It also populates the attributes of the unmanaged address in the editor. Enter the appropriate information in the editor.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

**Note:** After the conversion, the status of the unmanaged address changes to **Used**.

The following are some conditions for a conversion:

- **A and AAAA records:** You must select a DNS zone when converting an unmanaged address to an A or AAAA record.
- **PTR record:** You must select a DNS zone when converting an unmanaged address to a PTR record.
- **IPv4 and IPv6 Fixed Address:** Grid Manager displays a confirmation dialog box to ensure that you want to create a fixed address for the unmanaged address.
- **IPv4 and IPv6 Host record:** You can use the unmanaged address to enable a host record for DNS or DHCP.

### Clearing Unmanaged Data

Unmanaged objects are objects that are not configured for DNS or DHCP and do not have any corresponding NIOS objects such as fixed addresses, DNS records, or host records. You can clear unmanaged data if you do not want it to appear in the discovered data. Any unmanaged data that was discovered in a previous discovery can be removed. When you clear an unmanaged IP address, the status of the IP address changes to **Unused**.

Note that for cloud deployments, you can remove an unmanaged VM only when all the VM related properties are removed first. When the VM is removed, the tenant pointing to this VM will also be removed automatically. For information about cloud deployments, see [Deploying Cloud Network Automation](#).

To clear unmanaged data:

1. For **IP addresses:** From the **Data Management** tab -> **IPAM** tab, select an unmanaged IP address in the **IP Map or List** panel.
   For **networks:** From the **Data Management** tab -> **IPAM** tab -> **IP Map or List** panel, select a network in which you want to clear all unmanaged addresses.
   For **Cloud tenants:** From the **Cloud** tab -> **Tenants** tab, select a tenant for which you want to clear unmanaged data.
   For **Cloud VMs:** From the **Cloud** tab -> **VMs** tab, select a VM for which you want to clear unmanaged data.

2. Click **Clear** -> **Clear Unmanaged Data** or **Clear All Unmanaged Data** from the Toolbar.

3. In the **Clear Unmanaged Data** confirmation dialog box, click **Yes**. The appliance clears data that has no corresponding NIOS objects such as fixed addresses, DNS records, or host records.

**Note:** When you clear unmanaged addresses in a given network view, all unmanaged IPv4 and IPv6 addresses of all networks in the network view are cleared. When you select an entire network or a specific network in the **IP Map or List** panel, all the unmanaged addresses in the network are cleared. After you clear the unmanaged data, the status of the IP addresses changes to **Unused**.

### Resolving Conflicting Addresses

Conflicts happen when discovered data does not match existing IP address data. The **IP Map** panel and the **Cloud** tab -> **VMs** tab display conflicting addresses with a red background. The **IP List** panel displays **Conflict** as the status for all conflicting addresses. For objects that have multiple conflicts, Grid Manager lists each of them in a bulleted list in the **Resolve multiple conflicts** dialog. You can select a conflict, in any order, to begin resolving each issue. After you resolve the selected issue, Grid Manager returns to the **Resolve multiple conflicts** dialog so you can resolve other issues.

Depending on the conflict, you can do one of the following to resolve it:

- For a DHCP lease conflict, you can clear the existing lease and create either a fixed address or a reservation for the IP address. You can also keep the existing data and clear the discovered data. For information, see [Resolving DHCP Lease Conflicts](#).
- For a fixed address conflict, you can either keep the existing fixed address data or update the existing data with the discovered data. For information, see [Resolving Fixed Address Conflicts](#).
- For a DHCP range conflict, you can create a fixed address, create a reservation, or clear the discovered data. For information, see [Resolving DHCP Range Conflicts](#).
- For a host conflict, you can either keep the existing host record data or update the existing data with the discovered data. For information, see [Resolving Host Conflicts](#).
- For a VM affiliation conflict, you can either update all the displayed objects to be affiliate with the discovered data or keep the current affiliation and clear the conflict. For information, see [Resolving VM Affiliation Conflicts](#).

You must resolve conflicting addresses individually. You cannot resolve multiple conflicts at the same time.

**Note:** Once the conflict is resolved, the status of the IP address changes depending on how you resolved the conflict.

To resolve a conflict:

1. In the **IP Map or List** panel, select a conflicting address, and then click **Resolve Conflict** from the Toolbar.
2. The **Resolve Conflict** dialog box displays the reason of the conflict and lists the existing information and discovered information of the address in the **Description** field. Depending on the type of conflict, the appliance displays the corresponding resolution options. You can
compare the existing and discovered data and decide how you want to resolve the conflict.

Resolving DHCP Lease Conflicts

When an IP address has a DHCP lease and the discovered MAC address is in conflict with the existing MAC address, the IP address has a DHCP lease conflict.
To resolve a DHCP lease conflict:

1. In the Resolve Conflict or Resolve multiple conflicts dialog, Grid Manager displays the nature of the conflict and the discovered data versus the current data. Select one of the following to resolve the conflict:
   - Clear lease and create fixed address from discovered data: Clears the existing DHCP lease and creates a fixed address with the discovered data. The Fixed Address editor appears with the discovered data populated.
   - Clear lease and create a reservation from discovered data: Clears the existing DHCP lease and creates a new reservation using the discovered data. The Reservation editor appears with the discovered data populated.
   - Keep the existing and ignore this conflict: Keeps the current DHCP lease for the address and ignores the lease conflict.
2. Click OK or Resolve (when you have multiple conflicts). If you have multiple conflicts, Grid Manager returns to the Resolve multiple conflicts dialog so you can resolve other conflicts.

Resolving Fixed Address Conflicts

When the discovered MAC address of an IPv4 address does not match its existing MAC address, or when the DUID of an IPv6 address does not match its existing DUID, the IP address has a fixed address conflict.
To resolve a fixed address conflict:

1. In the Resolve Conflict or Resolve multiple conflicts dialog, Grid Manager displays the nature of the conflict and the discovered data versus the current data. Select one of the following to resolve the conflict:
   - Keep fixed address and clear discovered data: Keeps the existing fixed address and clears the discovered data.
   - Update fixed address with discovered data: Updates the existing fixed address data with the discovered data.
2. Click OK or Resolve (when you have multiple conflicts). If you have multiple conflicts, Grid Manager returns to the Resolve multiple conflicts dialog so you can resolve other conflicts.

Resolving DHCP Range Conflicts

When an IP address is in a DHCP range and does not match an existing DHCP lease, fixed address, or exclusion range and it shows an active state during a discovery, the IP address has a DHCP range conflict.
To resolve a DHCP range conflict:

1. In the Resolve Conflict or Resolve multiple conflicts dialog, Grid Manager displays the nature of the conflict and the discovered data versus the current data. Select one of the following to resolve the conflict:
   - Create a fixed address: Creates a fixed address with the discovered data.
     If the fixed address is served by a Microsoft server, but is outside of a scope, you must then navigate to the Fixed Address editor and assign the fixed address to the appropriate Microsoft server.
   - Create a reservation: Creates a reservation with the discovered data. This creates an Infoblox reservation and therefore cannot be used for IP addresses served by Microsoft servers. Note that you cannot convert an IPv6 address to a reservation.
   - Clear discovered data: Clears the discovered data and no object is created for the IP address.
2. Click OK or Resolve (when you have multiple conflicts). If you have multiple conflicts, Grid Manager returns to the Resolve multiple conflicts dialog so you can resolve other conflicts.

Resolving Host Conflicts

When the MAC address of an IPv4 address that belongs to a host record does not match its existing MAC address, or when the DUID of an IPv6 address that belongs to a host record does not match its existing DUID, the IP address has a host conflict.

1. In the Resolve Conflict or Resolve multiple conflicts dialog, Grid Manager displays the nature of the conflict and the discovered data versus the current data. Select one of the following to resolve the conflict:
   - Keep host record and clear discovered data: Keeps the existing data and clears the discovered data.
   - Update host record with discovered data: Updates the existing host record data with the discovered data.
2. Click OK or Resolve (when you have multiple conflicts). If you have multiple conflicts, Grid Manager returns to the Resolve multiple conflicts dialog so you can resolve other conflicts.

Resolving VM Affiliation Conflicts

When an IP address contains objects that are affiliated with a VM that is not the same as the discovered VM, this IP address has a VM affiliation conflict.
To resolve a VM affiliation conflict:

1. In the Resolve Conflict or Resolve multiple conflicts dialog, Grid Manager displays the nature of the conflict and the discovered affiliation versus the current affiliation. Select one of the following to resolve the conflict:
   - **Update all the displayed objects to be affiliate to the discovered affiliation**: Update all associated objects in this IP address to affiliate with the discovered affiliation.
   - **Keep the current affiliation(s) and clear the conflict**: Keeps the existing data and clear the conflict.
2. Click OK or Resolve (when you have multiple conflicts). If you have multiple conflicts, Grid Manager returns to the Resolve multiple conflicts dialog so you can resolve other conflicts.

Resolving MAC Address Conflicts

When the MAC address of an existing IP address does not match the MAC address of the discovered data, the object has a MAC address conflict.

To resolve a MAC address conflict:

1. In the Resolve Conflict or Resolve multiple conflicts dialog, Grid Manager displays the nature of the conflict and the discovered data versus the current data. Select one of the following to resolve the conflict:
   - **Change the configured MAC address to the same as the discovered MAC address**: Change the MAC address to the discovered MAC address.
   - **Keep fixed address and ignore this conflict**: Keep the fixed address and ignore the discovered data.
2. Click OK or Resolve (when you have multiple conflicts). If you have multiple conflicts, Grid Manager returns to the Resolve multiple conflicts dialog so you can resolve other conflicts.

Clearing Discovered Data

You can clear previously discovered managed data for selected IPv4 or IPv6 networks. This action is useful, for example, if your network topology has changed since the last discovery and you want to discover new data on the network or cloud platform. You may perform this action whether or not the network is in a managed or unmanaged state.

**Note:** This action clears only the discovered data that is supported in the Discovered Data section for an IP address. It does not clear any NIOS objects or information such as tenants, networks, or VMs for a cloud platform. If a discovered IP address has the same IP as an existing NIOS object (such as a fixed address, DNS record, or host record), the appliance removes this IP address.

To clear discovered data:

1. In the IP Map or List panel, select a network, and then click Clear -> Clear Discovered Data from the Toolbar.
2. In the Clear Discovered Data dialog box, click Yes.

You can also clear discovered data on all networks in a network view as follows:

1. In the IP Map or List panel, select a network, and then click Clear -> Clear Discovered Data from the Toolbar.
2. In the Clear Discovered Data dialog box, click Yes.

**Note:** When you clear all discovered data in a given network view, all imported discovered data for managed addresses in all IPv4 and IPv6 networks in the network view are cleared.

You can also clear discovered data for a specific discovery job, as follows:

1. From the Cloud tab -> VM tab, select Discovery Manager from the Toolbar.
2. In the vDiscovery Job Manager dialog, click the Action icon (shown as a gear in each row) next to the selected vDiscovery job, and then select Clear Discovered Data.
3. In the Clear Discovered Data dialog box, click Yes. The appliance clears all the discovered managed data that is collected by the specified vDiscovery job.

Clearing All Discovery Data

You can clear all the discovered data, whether managed or unmanaged, for a specific vDiscovery job. This action removes only the discovered data, not the associated NIOS objects, collected by the specified vDiscovery job only. It does not remove any discovered data collected through Network Insight or other non vDiscovery tasks.

**Note:** If the same data is collected by the specified vDiscovery job and another non vDiscovery job such as Network Insight or IP discovery, the discovered data remains intact and will not be removed.

To clear all discovered data for a specific vDiscovery job, do the following:
1. From the **Cloud** tab -> **VM** tab, select **Discovery Manager** from the Toolbar.
2. In the vDiscovery Job Manager dialog, click the Action icon (shown as a gear in each row) next to the selected vDiscovery job, and then select **Clear All Discovery Data**.
3. In the **Clear Discovered Data** dialog box, click **Yes**. The appliance clears all the discovered managed and unmanaged data that is discovered by the specified vDiscovery job.

### Integrating Discovered Data From NetMRI

The NetMRI appliances discover and track IPv4 and IPv6 network devices and provide information about the discovered IP addresses. You can integrate IPv4 and IPv6 discovered data into the NIOS appliance database, and then view the data in the IP List panel of Grid Manager as well as in the **Discovered Data** tab of certain IPAM object editor. When you start synchronization of discovered data from the NetMRI appliance, only the available IP addresses in the network are discovered. The imported data from the NetMRI appliance can only be modified or deleted by the specific synchronization. When you import the discovered data again for the same network and if some of the information in the network is changed, the newly discovered data and the originally discovered data (now old data) co-exist in the database. When you import the data again, the old data is deleted or modified, or the new data is added depending on the information discovered. For information about NetMRI IP discovery and how to import discovered data from a NetMRI appliance to the NIOS appliance, refer to the **Infoblox NetMRI Administrator Guide**.

**Note:** The NIOS appliance does not import IPv6 leases that contain prefixes and link-local IPv6 addresses. This data is discarded during an import.

The appliance can import the following IPv4 and IPv6 data that NetMRI discovers:

- **IP Address:** The discovered IPv4 or IPv6 address.
- **Discovered MAC Address:** The MAC address of the discovered host.
- **Last Discovered:** The date and time the IP address was last discovered.
- **NetBIOS Name:** The name returned in the NetBIOS reply or the name you manually register for the discovered host.
- **OS:** The operating system of the detected host.
- **First Discovered:** The date and time the IP address was first discovered.
- **Discoverer:** Specifies whether the IP address was discovered by a NetMRI discovery process.
- **Attached Device Description:** A textual description of the network device associated with the discovered IP address.
- **Attached Device Address:** The IP address of the switch that is connected to the end device.
- **Attached Device Name:** The name returned in the NetBIOS reply or the name you manually register for the discovered host.
- **Attached Device Port Description:** A textual description of the switch port that is connected to the end device.
- **Attached Device Port Name:** The name of the switch port connected to the end device.
- **Attached Device Port:** The number of the switch port connected to the end device.
- **Port Duplex:** The negotiated or operational duplex setting of the switch port connected to the end device.
- **Port Link:** The link status of the switch port connected to the end device. Indicates whether it is connected.
- **Port Speed:** The link speed, in Mbps, of the switch port.
- **Port Status:** The link status of the switch port. Indicates whether the port is up or down.
- **VLAN Name:** The name of the VLAN of the switch port.
- **VLAN:** The ID of the VLAN of the switch port.

### Chapter 15 Infoblox Network Insight

This chapter provides information about Infoblox Network Insight, which unites network discovery for geographically dispersed networks, infrastructure devices and network assets with the Infoblox IPAM (IP Address Management) solution. Through discovery, Network Insight provides automated, comprehensive, and accurate data about your network devices and their attributes so you can have better visibility in your network infrastructure, including the virtual network infrastructure, and manage it more efficiently.

This chapter describes how you use Network Insight to detect and manage information about network infrastructure devices, how to provision and de-provision networks, and how to manage and provision device ports, including switched Ethernet.

It includes the following sections:

- **About Network Insight**
  - Consolidator and Probes
  - Deployment Guidelines for Consolidator and Probes
  - Supported Discovery Methods
  - Starting Discovery
  - Managing Discovery
- **Discovering VRF Virtual Networks**
  - Special Considerations for Managing VRF Virtual Networks
  - VRF Deployment Guidelines
- **Administrative Permissions for Discovery**
- **Defining the Discovery Member Type**
- **Mapping Discovery Interfaces to Network Views**
- **Starting and Stopping the Discovery Service**
- **Starting the Discovery Service**
- **Stopping the Discovery Service**
• Configuring Discovery Properties
  • Defining Basic Polling Settings for the Grid
  • Defining Advanced Polling Settings for the Grid
  • Configuring SNMP1/v2 Credentials for Polling
  • Configuring SNMPv3 Properties
  • Configuring CLI Discovery Properties
  • Defining CLI Credentials Settings for Objects
  • Testing SNMP and CLI Credentials
  • Defining Seed Routers for Probe Members
• Configuring Automatic VRF Mapping
• Excluding IP Addresses from Discovery
  • Quick Exclusion of IPs from Discovery
  • Creating a New IPAM Object and Excluding it from Discovery
  • Excluding IP Addresses in Grid Manager
• Discovering Devices and Networks
  • Using Discover Now to Discover an Existing Object
  • Smart Folders and Discovered Devices
  • Using the Device Selector
  • Tips for Quick Navigation
• Managing Discovered Data
  • Converting Unmanaged Devices to Managed Devices
  • Converting Unmanaged Networks to Managed Status
  • Converting Unmanaged Networks under IPAM to Managed Status
  • Converting Unmanaged IP Addresses to Managed Status
  • Converting Unmanaged Assets to Managed Status
• About Automatic Conversion Rules
  • Configuring Automatic Conversion Rules
  • Supported Conversion Parameters
• Viewing Discovered Devices and their Properties
  • Viewing the Complete List of Discovered Devices
  • Viewing Discovered VRFs and Mapping Network Views
• Accessing Detailed Device Information
  • Viewing Interface Information for Discovered Devices
  • Determining Interface Capabilities
  • Viewing Networks Associated with Discovered Devices
  • Modifying Networks
  • Viewing IP Addresses Associated with Discovered Devices
  • Viewing Router Redundancy Information
  • Viewing Assets Associated with Discovered Devices
  • Viewing Components of Discovered and Managed Devices
• Viewing Discovery Status
  • Analyzing Discovery Status
• Executing Discovery Diagnostics
  • Viewing the Management State of IPs in Discovered Networks
• Disabling Discovery for a Network
• Adding Discovery Device Support
• Port Control Features in Network Insight
  • About Port Reservations
• Editing Interfaces in a Device
  • Editing Multiple Interfaces
  • Editing Multiple Interfaces from the Devices Page
  • Inline Interface Editing
• Provisioning and De-Provisioning Networks
  • De-provisioning Networks
  • Troubleshooting Port Control Tasks
• Creating Port Reservations for IPAM Objects
  • Editing Port Reservation Settings for IPAM Objects
  • Defining Port Reservations for an Infoblox Grid Member
  • Defining Port Reservations for an HA Pair
  • Editing Port Reservation Settings for an Infoblox Grid Member
  • Defining Device Information
• Defining Blackout Periods
  • Defining Blackout Periods for the Grid
  • Defining Blackout Periods for Networks
• Defining Port Configuration Blackout Periods
  • Defining Port Configuration Blackouts for the Grid
  • Defining Port Configuration Blackouts for Networks
• Conflict Resolution in Network Insight
  • Resolving Port Reservation Conflicts
  • Resolving Multiple Conflicts
About Network Insight

Infoblox Network Insight provides discovery features for detecting and managing devices in your network infrastructure. You can use discovery to collect device data and manage it through Grid Manager. For more information about device management, see Managing Discovered Data. You can view the operating state of all discovered network infrastructure devices and newly discovered IP networks, including but not limited to routers, firewalls, load balancers, Ethernet L2/L3 switches, end hosts, end host networks, VRF (Virtual Routing and Forwarding) virtual networks, and single and multipoint VPNs. Network Insight makes it easy to manage and secure your enterprise network by detecting all interfaces for every discovered device and providing specific information about them. For information about discovering VRF virtual networks, see Discovering VRF Virtual Networks.

The Infoblox IPAM feature set also provides control mechanisms by including and excluding networks and IP addresses for discovery. You can schedule and define when discovery takes place on any network, and define blackout periods during which no discovery tasks occur. Infoblox IPAM and DHCP functions also extend network control to assigning of discovered switch and router interfaces to IPAM objects such as IP networks, IP reservations, and host records. The assignments are called port reservations and are part of a feature set called port management, managed through Grid Manager. For more information, see Port Control Features in Network Insight.

Infoblox provides a few reports in which you can view trending information about the device groups, types of devices, and device IP addresses for the devices that are discovered by Network Insight. For information about these reports, see Network Insight Dashboards.

Supported Appliances for Network Insight

Network Insight is supported on the following physical appliances: ND-800, ND-805, ND-1400, ND-1405, ND-2200, ND-2205, and ND-4005; and the following virtual appliances: ND-V800, ND-805, ND-1400, ND-V1405, ND-V2200, ND-V2205, and ND-V4005. All appliances that perform discovery require a Discovery license. Appliances with this license only perform discovery tasks and do not perform core DNS or DHCP functions.

Discovery appliances that only detect devices and collect device data are called Probes, which are members of the Infoblox Grid, separately dedicated to the tasks of polling and discovery of networks and devices. A separate appliance, called the Consolidator, aggregates and organizes all collected device information from the Probes and synchronizes with the Grid Master. For more information, see Consolidator and Probes.

You can configure supported appliances as the Consolidator and Probes, as illustrated in Figure 15.1. The Consolidator aggregates discovered data it collects from Probes and transfers the data to the Grid Master for device management and reporting purposes.

In the Grid, the Grid Master synchronizes data among all Grid members through encrypted VPN tunnels. Communications between the Consolidator and Probes are also through encrypted VPN tunnels. The default source and destination UDP port number for VPN tunnels in a Grid is 1194. You can use the default port number or change it for VPN communications. Note that all the VPN tunnels in the Grid use the same port number you have chosen.

Figure 15.1 Network Insight Appliances Added as Grid members

Network Insight appliances use SNMP and other protocols to discover and catalogue a diverse assortment of device types, including the following: routers, enterprise switches, firewalls and security appliances, load balancers, enterprise printers, wireless access points, VoIP concentrators, application servers, VRF-based virtual networks, and end hosts.

Network Insight provides a tool for administrators to gather key information about networks, including the discovery of routed paths and the host clouds behind enterprise switches, even in organizations where an Infoblox deployment already exists. In Figure 15.2, an appliance running discovery connects to an enterprise router, and uses its information to determine more about the networks that exist deeper within the unmanaged network, termed the discovery domain in this example.

Figure 15.2 Discovery in Action
As indicated in Figure 15.2, discovery can trace through multiple hops and perform device discovery at every step, filling out the maps of unmanaged networks for the administrator.

The collection of unmanaged network information extends to the networks of distribution Ethernet switches. Data collection also includes end hosts and application/file servers connected to edge switches in enterprise offices. Discovery uses the term assets to describe these devices. For more information, see Viewing Assets Associated with Discovered Devices.

The Probes return discovery data to the Consolidator, which synchronizes device information with the Grid Master. Once information about discovered devices and networks resides on the Grid Master, you can convert unmanaged networks and devices to managed objects, adding them to the NIOS database. For more information, see Managing Discovered Data and About Automatic Conversion Rules.

You can also configure the appliance to send SNMP and email notifications when it discovers unmanaged devices and networks. For information about how to enable SNMP and email notifications for discovered unmanaged objects, see Setting SNMP and Email Notifications. You can also manage these notifications by configuring the maximum number of unmanaged objects the appliance detects before it sends notifications and how often it notifies about these events. For information about how to configure these parameters, see Defining Seed Routers for Probe Members.

You provide one or more routers as seed routers to act as the initial gateways for discovering other networks and their devices in the discovery domain (an example appears in Figure 15.2). You can also use DHCP routers (e.g., routers serving DHCP leases) as seed routers to aid in faster discovery.

When you create new networks, you can optionally provision them onto devices and perform discovery on them. Once you create the network, discovery can locate, poll and catalogue the network devices comprising the networks. This information is then synchronized with the Grid Master. For more information, see Discovering Devices and Networks.

Note: For comprehensive coverage of port control features in Grid Manager, see Port Control Features in Network Insight and its various subsections.

You can also exclude networks and IP addresses from discovery. The basic principle is that some devices do not need to be discovered, perhaps because they are already managed as part of a Grid and hence should not be subjected to discovery; because a device does not support SNMP; or for other organizational reasons. In Figure 15.2, networks 172.16.2.0/24 and 172.16.3.0/23 are excluded from discovery because they are already fully managed by a Grid. For more information, see Excluding IP Addresses from Discovery.

You can define scheduled time periods in which Network Insight does not perform discovery operations in the network. These time periods are called discovery blackouts. All protocols associated with discovery (SNMP, CLI through Telnet and SSH, port scanning, fingerprinting and Ping sweeps) can be shut off during discovery blackout periods. This prevents discovery protocols from occupying network bandwidth during periods of peak usage. Network Insight does not communicate with devices in any way during a discovery blackout period. For more information on discovery blackouts, see Defining Blackout Periods. Network Insight also provides a second type of blackout period for port configuration tasks, during which no tasks to change device port settings will execute. For more information, see Defining Port Configuration Blackout Periods.

Consolidator and Probes

Consolidator—The central repository of discovery data for the entire managed network. The Consolidator is a single appliance that contains data about all devices detected through discovery. The Consolidator communicates with the Grid Master as a normal Grid Member and transfers all its data to the Grid Master, as indicated in Figure 15.1. The Consolidator compiles information from one or more associated Probe appliances. The Consolidator appliance requires the Discovery license. If you have one or more Probe appliances or virtual appliances, the Consolidator performs no discovery on its own. If you plan to use a single dedicated appliance for discovery, that appliance must be licensed for discovery and be configured as a Consolidator. Note that the Grid Master cannot be licensed as a Consolidator.

Probes—A Probe is a Network Insight appliance or virtual appliance that performs the direct querying, probing and polling of network devices and the initial data collection. Probe appliances also require the Discovery license.

Infoblox recommends using one or more Probe appliances with the Consolidator. Each Probe can override the Grid level discovery credentials with its own discovery credentials.

Data synchronization occurs continuously between the Consolidator and all associated Probe appliances and between the Consolidator and the Grid Master.
**Note:** You assign each Probe appliance to a single network view, and multiple Probe appliances can share the same network view. You can change network view assignments for Probe appliances at any time. On ND-1400, ND-1405, ND-2200, ND-2205, ND-4000, ND-V1400, ND-V1405, ND-V2200, and ND-V2205 Network Insight appliances, you can assign multiple VLAN interfaces on the same Probe to different network views.

**Consolidator-Probe Appliance**—You may also choose to operate a Consolidator-Probe appliance as a single discovery system. In this deployment, the appliance operates as both a Consolidator and a Probe, performs all discovery operations, aggregates all databases within it, and synchronizes with the Grid Master.

Standalone discovery appliances cannot be installed in a network that already has existing Probes and a Consolidator. For more information, see *Defining the Discovery Member Type* and *Mapping Discovery Interfaces to Network Views*.

### Deployment Guidelines for Consolidator and Probes

When you wish to install and deploy discovery appliances, use the following installation guidelines:

- **Installing a Standalone in the Grid**—Before you designate an appliance as a standalone discovery appliance, no previously installed Probes should be present on the network and joined to the Grid. If you install a new appliance intended as a standalone, in a network that already has one or more Probe instances (perhaps for testing or evaluation purposes), before discovery service is stopped on the Probe instances, the new “standalone” appliance automatically detects the Probe instances and starts as a Consolidator appliance, preventing it from acting to probe and detect devices as a standalone appliance. Consolidators cannot be assigned to network views or to discovery in network objects such as IPv4 or IPv6 network containers.

- **Converting a Consolidator to a Standalone**—Also consider the example of a Consolidator appliance operating with one or more instances running as Probes, each with respective Discovery licenses. If you wish to convert the Consolidator to a standalone discovery appliance, stop the discovery service on all associated probes. Then, stop and restart the discovery service on the Consolidator appliance. The appliance is selectable for discovery of network objects, acting as a standalone discovery appliance.

- **Adding new Probe Instances to a Standalone deployment**—Finally, consider the use of a standalone discovery appliance to which you wish to associate a new Probe instance or instances. This process converts a standalone to a Consolidator. After the new Probe instances join the Grid, stop the discovery service on the standalone discovery appliance. Then, start the discovery service on the new Probe or Probes. Next, restart the discovery service on the previously defined standalone appliance. It detects the newly active Probe instances and activates as a Consolidator.

- In all cases, you must maintain proper Discovery licensing.

### Supported Discovery Methods

When you perform a discovery, you can choose any or all of the following discovery methods:

- SNMPv1/v2c device polling as described in [SNMP](#).
- SNMPv3 device polling as described in [SNMP](#).
- CLI device querying as described in [CLI](#).
- ICMP Ping Sweep and Smart Subnet Ping Sweep as described in [ICMP](#).
- TCP as described in [TCP](#).
- NetBIOS as described in [NetBIOS](#).

These methods actively scan predefined networks and probe IP addresses. The appliance listens for responses from the IP addresses as proof of activity. The IP discovery scans through the specified network ranges and probes IP addresses (except for the network, broadcast, and multicast address types) in each network, including the /31 and /32 subnets. Note that addresses in the /31 and /32 subnets can be used only as source addresses for point-to-point links and loopbacks. In these cases, no broadcast or network addresses exist in the /31 and /32 subnets, and the appliance can discover source addresses in these subnets.

### SNMP

**Note:** Infoblox does not recommend using vendor default SNMP credentials on network devices. Should you need to use vendor defaults for a given device type, you enter those values in the list of SNMP credentials on the Grid Master.

Network Insight supports discovery of devices and networks through SNMPv1/v2c and through SNMPv3 protocols. Discovery acquires information from standard SNMP MIB object IDs (OIDs) to correctly identify and catalogue devices. You enter or import lists of SNMP credentials with which the appliances query devices on the network to perform discovery. SNMPv1 and SNMPv2c protocols are combined into a set termed **SNMPv1/v2** for discovery. SNMPv1/v2 discovery requires standard read community strings to be stored on the Grid Master.

Accounts using SNMPv3 use a standard suite of authentication and security protocols. If Network Insight uses SNMPv3 to collect data from devices supporting the protocol, you can define specific user credentials with combinations of authentication and protocol support, and the unique keys for each protocol. Network Insight also supports multiple entries for the same username string, enabling checking of similar SNMPv3 credentials that use different authentication and security protocols.

Some devices found by discovery may not have known SNMP credentials or credentials that are entered into the sets of SNMP credentials defined for discovery.

**Note:** SNMP Credentials from the Grid or from the Member credential list are always tried in the specified order unless a credential is associated with a host, fixed address or reservation being discovered.
CLI

Note: CLI is optional for discovery but is required for all Port Control operations. Discovery can perform CLI data collection to collect information for specific device types. SNMP is required for all device discovery.

Network Insight enables the use of dynamically created and closed Telnet and SSH command-line sessions to log in, query, and configure ports using each device's command-line syntax. Network Insight does so without requiring extensive configuration from the user. You need to provide known admin account login information and any Enable passwords for devices in the networks to be discovered. CLI credentials are required for port reservation and port configuration operations under Grid Manager. You enter CLI credentials under Grid Discovery Properties (Grid \rightarrow Grid Manager \rightarrow click Edit \rightarrow Grid Discovery Properties) to be inherited by discovery Probe members, and as necessary for each discovery Probe member. You can also override them for individual IPAM objects (fixed addresses, hosts and IPv4 reservations) and test the CLI credentials against devices for correctness. For more information, see Testing SNMP and CLI Credentials.

ICMP

Discovery uses different variations of Ping traces to perform higher-performance, brute-force device discovery. ICMP is the last resort when devices do not support SNMP management protocols or an SNMP credential is lacking. The ICMP Smart Ping Sweep option enables brute-force subnet Ping sweeps on IPv4 networks. Subnet ping sweeps are used as a last resort in the discovery process. A subnet ping sweep is performed if Network Insight is unable to identify any network devices in a given subnet. Subnet ping sweeps are performed no more that once per day, and will end the ping sweep on a given subnet once Network Insight discovers a network device and is able to collect data from it. You can configure the timeout value (Ping Sweep Timeout) and the number of attempts (Ping Sweep Attempts).

Note: Smart subnet ping sweeps are not performed on subnets larger than /22. Ping sweeps of any kind do not apply on IPv6 networks because of the greater scale of network addresses in the IPv6 realm.

Complete Ping Sweep differs from the Smart Subnet ping sweep in the following ways:

- The discovery ping sweep runs only against the specified range.
- The sweep runs regardless of the range size.
- The sweep runs regardless of the number of discovered devices within the specified range.

Discovery also performs automatic Ping traceroutes when needed for path collection. Path collections run without user intervention or configuration.

TCP

TCP scanning probes each active host on a list of TCP ports using TCP SYN packets. This method detects all active hosts that generate SYN ACK responses to at least one TCP SYN. The discovery can determine the OS on a host by analyzing how the host reacts to the requests on opened and closed ports. It then uses the TCP fingerprints to guess the OS. To obtain a TCP fingerprint, IP discovery provides two scanning techniques, SYN and CONNECT.

When you use the SYN technique, the discovery sends a TCP SYN packet to establish a connection on a TCP port. If the port is open, the host replies with a SYN ACK response. The discovery does not close the port connection. The CONNECT technique is a three-way TCP handshake. The discovery starts with the same process as the SYN technique by sending the TCP SYN packet. A response containing a RST flag indicates that the port is closed. If the host replies with a SYN ACK response, discovery sends a RST packet to close the connection. If there is no reply, the port is considered filtered. TCP scanning is a deliberate and accurate discovery method, enabling detection of all active hosts on a network provided that there are no firewalls blocking TCP packet exchanges.

You can choose the TCP ports and the TCP scanning technique in the Grid Discovery Properties editor. This method returns the following information for each detected host:

- **IP address**: The IP address of the host.
- **MAC address**: The discovery returns the MAC address only if the Probe member running the discovery is on the same discovered network.
- **OS**: This is set to the highest probable OS reported in the response.

To use the TCP discovery method, the TCP port and a specific set of ports between the Probe member and the discovered networks must be unfiltered. The default set of ports is defined by the factory settings.

TCP Port Scanning

By enabling port scanning, Network Insight probes the list of TCP ports enabled in the Advanced tab, to determine whether they are open. You can control some settings for port scanning behavior, including the choice of a TCP scanning technique.

- **Profile Device**: If enabled, Network Insight attempts to identify the network device based on the response characteristics of its TCP stack, and uses this information to determine the device type. In the absence of SNMP access, the Profile Device function is usually the only way to identify devices that do not support SNMP. If you disable Profile Device, devices accessible via SNMP are still correctly identified;
all other devices are assigned a device type of Unknown. Profile Device is disabled by default for discovery polling.

The Profile Device option uses the editable list of TCP protocol ports from the Grid Discovery Properties -> Polling -> Advanced tab as its profile, and polls each of the ports enabled in that list, using the configured timeout value and the number of polling attempts for each port. For more information, see Defining Seed Routers for Probe Members.

Should you disable Port Scanning, discovery attempts no port probes other than SNMP on any device.

NetBIOS

The NetBIOS method queries IP addresses for an existing NetBIOS service. This method detects active hosts by sending NetBIOS queries and listening for NetBIOS replies. It is a fast discovery that focuses on Microsoft hosts or non-Microsoft hosts that run NetBIOS services. NetBIOS discovery returns the following information for each detected host:

- IP address: The IP address of the host.
- MAC address: Listed only if the discovered host is running Microsoft, otherwise blank.
- OS: This value is set to Microsoft for an active host that has a MAC address in the NetBIOS reply.
- NetBIOS name: This value is set to the name returned in the NetBIOS reply.

To use the NetBIOS discovery method, ports 137 (UDP/TCP) and 139 (UDP/TCP) between the Grid member performing the discovery and the target networks must be unfiltered.

The following table summarizes the supported discovery methods:

<table>
<thead>
<tr>
<th>Discovery Type</th>
<th>Returned Data</th>
<th>Guideline</th>
<th>Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart IPv4 Subnet Ping Sweep</td>
<td>• IP address • MAC address</td>
<td>Apply on known subnetworks on which no devices are readily found. Limited to networks of /22 and smaller.</td>
<td>ICMP echo request and reply.</td>
</tr>
<tr>
<td>Complete Ping Sweep</td>
<td>• IP address • MAC address</td>
<td>Last resort for discovery. Use ICMP for a rough and fast discovery. Enables path tracing.</td>
<td>ICMP echo request and reply, ICMP traceroute.</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>• IP address • MAC address • OS • NetBIOS name</td>
<td>Use NetBIOS for discovering Microsoft networks or non-Microsoft networks that run some NetBIOS services</td>
<td>NetBIOS query and reply.</td>
</tr>
<tr>
<td>TCP</td>
<td>• IP address • MAC address • OS</td>
<td>Use TCP for an accurate but slow discovery</td>
<td>TCP SYN packet and SYN ACK packet.</td>
</tr>
<tr>
<td>Port Scanning/Profile Device</td>
<td>• Open and Closed TCP ports • IP Address</td>
<td>Disabled by default, use for non-SNMP devices.</td>
<td>Scans specified list of TCP ports, using TCP SYN packet.</td>
</tr>
<tr>
<td>SNMPv1/v2</td>
<td>• Open and Closed TCP ports • IP Address • System Description • System Up Time • Routing Neighbors • Routing and Forwarding Tables • ARP tables • SNMP credentials</td>
<td>Most important protocols for discovery. Ensure you have the SNMP credentials necessary for probing devices using SNMP.</td>
<td>Queries and collects system OIDs such as SysDescr and sysUpTime.</td>
</tr>
<tr>
<td>CLI (Device Command-Line by Telnet or SSH)</td>
<td>• Similar data set to SNMP • May be used instead of, or in combination with, SNMP</td>
<td>Requires correctly defined admin login tuples and Enable passwords where needed for device types. You may test credentials against devices and assign CLI credentials to individual objects, overriding Grid-level and Network-level credential settings.</td>
<td>Uses standard device-language scripts and configured Telnet or SSH connection settings to collect discovery data.</td>
</tr>
<tr>
<td>vDiscovery</td>
<td>• IP address • MAC address • OS • Discovered name • Virtual entity type • Virtual entity name • Virtual cluster • Virtual datacenter • Virtual switch • Virtual host • Virtual host adapter</td>
<td>Add the VMware vSphere servers on which you want to perform the vDiscovery. For information about how execute a vDiscovery, see Configuring vDiscovery Jobs.</td>
<td>The appliance communicates with the vSphere servers to collect discovery data on virtual machine instances.</td>
</tr>
</tbody>
</table>

Starting Discovery
To ensure a successful discovery, complete the following:

1. In the Grid, install valid Discovery licenses on the Network Insight supported members that will later become the Consolidator and Probes. For information about how to install licenses, see Managing Licenses.
2. When you join the discovery members to the Grid, the first member automatically becomes the Consolidator while the others become Probes. If you want to change the roles of these members after they join the Grid, you can re-define their member types, as described in Defining the Discovery Member Type. If you have only one discovery member, it automatically becomes the Consolidator-Probe appliance after it joins the Grid. For more information about the Consolidator and Probes, see Consolidator and Probes.
3. Configure applicable admin permissions for managing discovery and discovered data. For more information, see Administrative Permissions for Discovery.
4. Define discovery interfaces and map them to corresponding network views. This step is especially important for discovering VRF virtual networks. For more information, see Mapping Discovery Interfaces to Network Views.
5. Configure Grid discovery properties such as defining polling settings, configuring SNMP and CLI credentials, and configuring automatic VRF mapping. For more information, see Configuring Discovery Properties. Note that you can override the Grid settings at the member and network levels, except for automatic VRF mapping which can be configured only at the Grid level.
6. Optionally, you can configure seed routers and map them to the corresponding network views. You can also use the default gateways for associated DHCP ranges and networks as seed routers for discovery by selecting the Use DHCP Routers as Seed Routers in the General -> Advanced tab of the Grid Discovery Properties editor. For more information, see Defining Seed Routers for Probe Members and Defining Advanced Polling Settings for the Grid.

Note: You must map each discovery interface, seed, and VRF to its respective network view in order to have a successful discovery for virtual routing instances.

7. Specify a network view, network container, or network to be discovered. For more information, see Discovering Devices and Networks.
8. Optionally, define IP address exclusions when you want to exclude certain IPs from a discovery for various reasons. For more information, see Excluding IP Addresses from Discovery.
9. Define blackout periods when you do not want the appliance to perform discovery. For information about how to configure blackout periods, see Defining Blackout Periods.
10. Start the discovery service on the Consolidator and Probes to begin discovery, as described in Starting the Discovery Service. The Probe members continue to discover network devices within the defined networks.

Managing Discovery

After you start the discovery service, you can do the following to manage the discovery and discovered data:

- Monitor the discovery status, as described in Viewing Discovery Status.
- Execute discovery diagnostics to test the connection of a discovery member, as described in Executing Discovery Diagnostics.
- Stop discovery on a specific network, as described in Disabling Discovery for a Network.
- View a complete list of discovered devices, their associated interfaces, networks, IP addresses, assets, and components. For more information, see Viewing Discovered Devices and their Properties.
- Resolve conflicts for discovered data, as described in Conflict Resolution in Network Insight.
- Provision and de-provision networks and manage port configurations, as described in Port Control Features in Network Insight.

Discovering VRF Virtual Networks

You can configure Network Insight to discover network devices that are configured or deployed within VRF (Virtual Routing and Forwarding) virtual networks. Using Network Insight to discover virtual networks provides visibility into your entire virtual network infrastructure, which allows you to view and manage overlapping IP addresses, VRF-specific data, and discovered end hosts. Note that a virtual network can consist of one or more physical devices that are configured to route packets using separate and distinct routing processes. Multiple routing tables can coexist on the same physical device or virtual device context, and traffic is exchanged among those devices using multiple routing tables.

Depending on your network topology, there are a few ways you can use Network Insight for VRF network management. To use Network Insight effectively in the network, review the different deployment scenarios and configure Network Insight accordingly, as described in VRF Deployment Guidelines.

In addition, before you start a discovery for VRF virtual networks, ensure that you have reviewed the guidelines listed in Special Considerations for Managing VRF Virtual Networks.

Special Considerations for Managing VRF Virtual Networks

When you define discovery settings and perform management of VRF virtual networks, consider the following:

- If you limit the context of the SNMP community string in an individual VRF to the context of only that VRF, Network Insight will not be able to determine that the device it has discovered inside that VRF is the same device it has found inside other virtual networks. This may result in extra, un-correlated devices in the network. For information about how to configure SNMP credentials, see Configuring SNMP1/v2 Credentials for Polling and Configuring SNMPv3 Properties.
- Network Insight will become aware of some devices inside of virtual networks from the route and ARP tables of routers that it manages. Without network connectivity into those virtual networks through a virtual discovery interface, Network Insight cannot discover all the devices or manage them. To create the necessary connectivity, you must configure a Network Insight discovery interface to be part of the VRF.
- Network Insight collects and parses the ARP and routing information from within a VRF context, but this data will not be used for further discovery unless the VRF virtual network is associated with a network view that is mapped on a discovery interface. For more information...
about how to map network views to discovery interfaces, see *Mapping Discovery Interfaces to Network Views.*

- Global VRFs are labeled as: "default(IOS)" for IOS, "default" for Nexus and "master" for JunOS.
- For discovery and periodic polling on Juniper devices through an interface that is not in the Juniper default VRF (master), the query must use a special "default@credential" format. This setting assumes that users do not have management interfaces in a VRF. Your defined SNMP credentials for VRF-aware Juniper devices must use syntax similar to: "@credential". (Note that when querying VRF-aware Juniper devices via an interface that is in the default VRF, a plain community string can be used without the "@" character.)
- When configuring Network Insight to discover networks that employ route-leaking, discovery ranges for each network view should only be defined to include IP addresses that belong to that network view. In other words, any given Device IP should only fall within the discovery ranges of one network view. If discovery ranges are defined such that a device can be discovered by two different network views, the device may also be discovered via an unexpected network view. For information about how to define discovery ranges, see *Discovering Devices and Networks.*

**VRF Deployment Guidelines**

The topology of your network helps determine how you deploy Network Insight for VRF network management. To use Network Insight effectively in the network, you must possess some knowledge about your network so you can decide how to configure Network Insight to reach all the virtual networks you want to discover and manage. This section describes some common VRF-related network types for which you can deploy Network Insight.

Using the following three network types, all examples in this section help you define the number of network views and discovery interfaces so you can reach all locations in your network.

1. **VRF Network Type 1:** A network with a management VRF and several isolated production VRFs that include VRF-aware devices in the network.
2. **VRF Network Type 2:** A network with a shared service deployment VRF (shared VRF) and several isolated production VRFs that include VRF-aware devices in the network. The production VRFs share routes with the shared VRF, a practice also called route-leaking.
3. **VRF Network Type 3:** A network with several VRF-ignorant devices that reside in different L3 spaces, with no management VRF.

**VRF Network Type 1** has the following characteristics:

- A management VRF that reaches all VRF instances throughout the network.
- Isolated production VRFs (all VRFs can route to/from the management VRF but not to one another).
- The management VRF has complete visibility to all VRF instances in the network.

<table>
<thead>
<tr>
<th>Network Type 1</th>
<th>Management VRF</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RED VRF Network</td>
</tr>
<tr>
<td></td>
<td>Yellow VRF Network</td>
</tr>
<tr>
<td></td>
<td>Green VRF Network</td>
</tr>
<tr>
<td></td>
<td>= management interface</td>
</tr>
</tbody>
</table>

**VRF Network Type 2** has the following characteristics:

- Uses a shared services deployment VRF to offer network services to the other production VRFs (shared VRF).
- All VRFs are reachable from the shared VRF, but VRFs cannot reach each other through the shared VRF or between each other.
- The production VRFs (Red, Yellow, Green) share routes with the shared services VRF (Blue).
- The shared VRF has complete visibility to all VRF instances.

<table>
<thead>
<tr>
<th>Network Type 2</th>
<th>Shared VRF</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Red VRF Network</td>
</tr>
<tr>
<td></td>
<td>Yellow VRF Network</td>
</tr>
<tr>
<td></td>
<td>Green VRF Network</td>
</tr>
<tr>
<td></td>
<td>- Management intf.</td>
</tr>
<tr>
<td></td>
<td>Route Sharing</td>
</tr>
</tbody>
</table>

VRF Network Type 3 has the following characteristics:

- Devices have management IPs only inside their respective networks.
- The routers in the network are VRF-aware; the switches are VRF-ignorant.
Defining Network Views and Discovery Interfaces

In all three deployment types, you decide whether you want one or multiple network views based on how your network operates, as outlined in the three network types above. You can also consider the following guidelines:

- When all infrastructure devices for the network are reachable through a management VRF or a shared services VRF, and you do not need extended discovery capabilities to discover and/or manage end hosts, you can use a single network view. You also use a single virtual discovery interface to connect to the same 802.1q ID as the management VRF network. You can then discover and analyze all VRF-aware devices on the management VRF.
- If you want your devices end host and downstream device information separated for viewing and reporting, then you will want to use network views for each virtual network. Doing so is helpful for visual purposes, but it is not required.
- If you want ping sweeps, port scanning, fingerprinting and other discovery services into end hosts within each of your VRF networks, you must define multiple network views, one for each of your VRF networks; and each of which requires an associated virtual discovery interface and discovery ranges.

Deploying Network Insight in VRF Network Type 1: All Devices on a Management Network

The following figure shows an example of integrating Network Insight with Network Type 1. In this network deployment type, a single virtual discovery interface can manage all VRF instances' identification of ARP entries, because Network Insight needs only one discovery interface into the Management VRF.
Network Type 1:
All VRFs reachable from management VRF but VRFs cannot reach each other
(all VRFs can route to/from management VRF but not to each other).
Management VRF has complete visibility for each VRF.

Management VRF
Red VRF Network
Yellow VRF Network
Green VRF Network

Network Insight
= management interface

End Hosts

Network Insight
You configure the following for this example:

- **Network View**: Create one network view for the management VRF.
- **Discovery Interface**: Add the active discovery interface to the management VRF and tag it with the corresponding 802.1q VLAN value.
- **Discovery Ranges**: Define IP discovery ranges for the management network.
- All discovered VRFs must be associated with the network view configured for the management VRF.

Deploying Network Insight in VRF Network Type 1: All Devices on a Management Network (Part 2)

The following figure shows the same topology for Network Type 1, but using multiple discovery interfaces and multiple network views.

In this example, the switch must be configured with the trunk port 'facing' Network Insight to forward Network Insight's tagged 802.1q traffic to the appropriate destination networks (VLAN 5, VLAN 10, VLAN 20 and VLAN 30 in this example).

The encapsulated sub-interfaces are defined using the correct values on each port; the virtual discovery interfaces on Network Insight match these values.
Network Type 1, with Multiple Network Views and Scan Interfaces
Steps for Deployment:
- Configure Switch interfaces as Trunks
- Define 802.1q subinterfaces on Routers
- Multiple virtual scan interfaces on NetMRI (dot1q tags 5,10,20,30)

Network Insight

Management VRF
Red VRF Network
Yellow VRF Network
Green VRF Network
= management intf.

Network Insight

You configure the following for this example:

- **Network Views**: Create a network view for each network (Management, Red, Yellow, Green).
- **Discovery Interfaces**: Create virtual discovery interfaces for each VRF network.
- **Discovery Ranges**: Define IP discovery ranges for each VRF network.
- The discovered VRF instances must be associated with the network views to which they belong. For more information, see Viewing Discovered VRFs and Mapping Network Views.

Deploying Network Insight in VRF Network Type 2: All VRFs Reachable from a Shared Services VRF

This example illustrates the use of a shared service VRF between the distribution routers in the network and how Network Insight integrates into such a topology.
All virtual networks are reachable through a shared VRF, to which Network Insight may connect using a single virtual discovery interface and reach all other VRFs from the one to which it is connected. Each Router in this topology also shares routes between the VRFs.

**Network Type 2:**

<table>
<thead>
<tr>
<th>All VRFs reachable from shared VRF but VRFs cannot reach each other</th>
</tr>
</thead>
<tbody>
<tr>
<td>The VRFs share routes with the Shared VRF, which has complete visibility to each VRF.</td>
</tr>
<tr>
<td>Shared VRF</td>
</tr>
<tr>
<td>Red VRF Network</td>
</tr>
<tr>
<td>Yellow VRF Network</td>
</tr>
<tr>
<td>Green VRF Network</td>
</tr>
<tr>
<td>= Management intf</td>
</tr>
<tr>
<td>Route Sharing</td>
</tr>
</tbody>
</table>

You configure the following for this example:

- **Network View**: Use one network view for the shared VRF.
- **Discovery Interface**: Create a virtual discovery interface on the network view. Use a single virtual discovery interface in Network Insight, and connect through the facing switch to the shared VRF using the tagged 802.1q value. There is a 1:1 ratio between network views and discovery interfaces.
- **Discovery Ranges**: Define IP discovery ranges in the single network view for all VRFs.
- **All discovered VRFs must be associated with this network view.**

If you want your device end hosts and downstream devices information separated, then use network views for each virtual network. This is helpful for viewing and reporting but it is not required. In this example, only a single network view is applied.

**Deploying Network Insight in VRF Network Type 2: All VRFs Reachable from a Shared Services VRF (Part 2)**

In this version of the VRF Network Type 2 deployment, you use multiple network views and multiple discovery interfaces in a 1:1 ratio, with the same requirements for trunking and switch VLAN sub interfaces.
Network Type 2, with Multiple Network Views and Scan Interfaces
Steps for deployment:

Configure Switch Interfaces as Trunks
If data separation is needed, define 802.1q subinterfaces
Multiple virtual scan interfaces on Network Insight
(dottag 5,10,20,30) or single scan interface into switch.

Network Insight

Shared VRF
Red VRF Network
Yellow VRF Network
Green VRF Network

End Hosts  End Hosts  End Hosts  End Hosts

You configure the following for this example:

- **Network Views**: Create a network view for each network (e.g., Management, Red, Yellow, Green).
- **Discovery Interfaces**: Create virtual discovery interfaces for each VRF network.
- **Discovery Ranges**: Define IP discovery ranges in Network Insight for each VRF network.
- The discovered VRF instances must be associated with the network views to which they belong. For more information, see *Viewing Discovered VRFs and Mapping Network Views*.

Deploying Network Insight in VRF Network Type 3: Devices Reside in Disconnected Networks

In the final example, trunking is in use between Network Insight and its facing gateway switch into the managed network. This topology requires the use of multiple network views as all VRF networks are completely separate and cannot be reached through any management virtual network.
You configure the following for this example:

- **Network Views**: Create a network view for each network (e.g., Management, Red, Yellow, Green).
- **Discovery Interfaces**: Create virtual discovery interfaces for each VRF network.
- **Discovery Ranges**: Define IP discovery ranges for each VRF network.
- The discovered VRF instances must be associated with the network views to which they belong. For more information, see Viewing Discovered VRFs and Mapping Network Views.

Each of the network views requires a single virtual discovery interface using 802.1q tagging as indicated in the figure. When defining the virtual discovery interfaces, use the 802.1q tag from the network devices. The primary differences are as follows:

- All devices do not have a management IP address in the so-called management VRF.
- The routers are VRF-aware while the switches are not.
- No VRF shares routes between any of the VRFs.

### Administrative Permissions for Discovery

You can start a discovery and manage discovered data based on your administrative permissions. For more information, see About Administrative Permissions.

Initiating and controlling a discovery requires specific administrative permissions. The following are permission guidelines for initiating and controlling a discovery:

- The **IPAM Discovery Admin** role provides a pre-configured list of permissions by which assigned admin accounts may perform discovery tasks. Administrators with these permissions can initiate and control discovery on any existing network. By default, the IPAM Discovery Admin role supports the following permissions:
  - All permissions associated with the Network Discovery feature set (active if you do not have a Network Insight license)
• Read-Only on all Network Views, network containers, networks and ranges
• Read-Only on all hosts
• Read-Only on all Members
• Read-Write Network Discovery permissions
• Editing network, network container or range discovery properties: Read-Only for each type. For member assignment, the user also needs additional read-only permission for the assigned member
• Editing fixed address, host or reservation discovery properties: Read-only for each type
• Excluding an IP address or an IP Range (from the Network Editor’s Discovery Exclusions tab or from the IPAM IP List view): read-only permission for the network
• Defining discovery and port configuration blackouts at the Grid and Network levels
• Discover Now for Network, DHCP Range, IP address or device: Read-Only permission for each.

• If the user does not possess the Network Discovery permission, all Network Insight permissions and operations are disabled.
• A Port Control permission under the IPAM Permissions type allows you to add a Read/Write or Deny permission for a device; a network; a network container; or network view. You can also add a global RW/Deny port control permission for all network views.
  • If the user does not possess the Port Control permission, the user cannot provision networks, de-provision networks, perform port reservations or configure interfaces. All non-Superuser accounts must have the Port Control permission to create port control tasks for any affected objects.
• Superusers can initiate and control discovery on all networks. Some discovery functions require superuser permissions:
  • Grid Discovery properties
  • Uploading, Viewing and deletion of device support bundles
  • Launching Discovery Diagnostics
  • Launching Discovery Status

Similar to Network Discovery, devices and end hosts found through discovery can undergo conversion from unmanaged status to managed status. This entails converting an unmanaged IP address to a host, an A record or AAAA record, a PTR record, or to a fixed address.

• Administrators with read/write permission to a DNS zone or specific record type can convert unmanaged data to a host, fixed address, reservation, A record, or PTR record.
• IPAM Discovery admins can convert unmanaged networks to managed networks and can change discovery settings for networks.
• For unmanaged networks: users may Delete, Convert (to managed), Clear Unmanaged Data and Clear Discovered Data if one of the following is true:
  • User has read-write permission for the network
  •–or–
  • User has Network Discovery permission plus Read-Only for the network.

After a discovery is complete, the following permission guidelines apply to viewing and managing discovery data:

• Superusers can view and manage all discovered data.
• Administrators with read permission to networks can view all discovery data without editing.
• If a user has read-only permissions for a device’s management IP address, the device is visible in the Data Management –> Devices tab.

For more information on configuring admin user accounts and working with permissions, see the sections under Managing Administrators. For information about discovery permissions, see Administrative Permissions for Network Insight Tasks.

**Starting and Stopping the Discovery Service**

**Note:** The discovery service can only be started on Grid members that are configured as the Consolidator or Probe (i.e. the Grid members with valid Discovery installed).

Each discovery member requires separate Discovery licenses, and must have a running discovery service. Consider the following before starting or stopping the discovery service:

• The Grid Master does not run the discovery service.
• Appliances running a Discovery license and the discovery service do not support HA pairs.
• Discovery Probe appliances appear as Grid members in Grid Manager.
• All appliances running discovery must have the Discovery license installed before starting the service.
• Appliances running discovery do not run core network services such as DNS and DHCP. Discovery appliances may also run the NTP service.
• If you expect to run a single appliance in the Grid for discovery, the appliance is designated as a Consolidator, and also performs Probe discovery operations.
• When you add a new Grid member with a Discovery license, the appliance is set automatically to the following:
  • A Consolidator, if no other discovery member exists in the Grid.
  • A Probe, when at least one discovery appliance exists in the Grid

**Note:** When a member joins the Grid and applies a Discovery license for the first time, the admin user needs to log off and log in again to Grid Manager to see the discovery-enabled functionality.

For information about discovery configuration at the service level, see Configuring Discovery Properties.
Starting the Discovery Service

To start the discovery service on a licensed Consolidator or Probe appliance:

1. From the Grid tab, select the Grid Manager tab, and click the Services tab.
2. Click the Discovery icon to display the list of members running the discovery service.
3. Select the discovery member or members for which you wish to start the service.
4. Expand the Toolbar and click Start.
   The appliance asks you to verify that you want to proceed with starting the service for the selected member.
5. Click Yes.

Stopping the Discovery Service

To stop the discovery service on the Consolidator or Probe appliance:

1. From the Grid tab, select the Grid Manager tab, and click the Services tab.
2. Click the Discovery icon to display the list of members running the discovery service.
3. Select the discovery member or members for which you wish to stop the service.
4. Expand the Toolbar and click Stop.
   The appliance asks you to verify that you want to proceed with stopping the service for the selected member.
5. Click Yes.

Defining the Discovery Member Type

Before using Network Insight to discover devices and networks, you must first define the consolidator and probes in your Grid and specify the discovery interfaces on these members. For information about how to map discovery interfaces to network views, see Mapping Discovery Interfaces to Network Views. Note that when you first join a discovery member to the Grid, the first discovery member that joins the Grid automatically becomes the Consolidator and all other discovery members become Probes. If you have only one discovery member in the Grid, it becomes the Consolidator-Probe standalone discovery appliance.

On some occasions, you may wish to change an appliance with a Discovery license to a Consolidator or to a Probe, or change a Consolidator to a standalone discovery appliance. To make any of these changes, you must first stop the discovery service on the appliance. For more information, see Starting and Stopping the Discovery Service.

To define the discovery appliance type:

1. From the Grid tab, select the Grid Manager tab, and click the Services tab.
2. Click the Discovery icon to display the list of members running the discovery service.
3. Select the discovery member for which you wish to change the appliance type.
4. Expand the Toolbar and click Edit -> Member Discovery Properties.
5. In the General tab of the Member Discovery Properties editor, choose the Member Type:
   - Polling: Turns the appliance into a discovery Probe appliance.
   - Consolidator: Turns the appliance into a discovery Consolidator appliance.
   - Unassigned: Disables the discovery feature on the appliance.

   Note: You cannot change the member type when the discovery service is running. Stop the discovery service first before changing the discovery member type.

6. Save the configuration. If you wish to change the interface over which the appliance sends and receives discovery traffic, see Mapping Discovery Interfaces to Network Views.

Mapping Discovery Interfaces to Network Views

Discovery Probe members must have a designated interface or interfaces over which all discovery traffic exchanges take place. You may designate one or multiple discovery interfaces on each Probe member. You can specify the LAN1, LAN2, MGMT, and VLAN ports as the discovery interfaces. These ports must first be defined in the member network settings before they can be used for discovery. Note that when you configure VLANs on Network Insight appliances, the VLANs are used for discovery only. They do not support other core network services. On ND-1400, ND-1405, ND-2200, ND-2205, ND-4000, ND-V1400, ND-V1405, ND-V2200, and ND-V2205 Network Insight appliances, you can assign multiple VLAN interfaces on the same Probe to different network views.

To discover VRF virtual networks, you must discover their corresponding routes. In order to identify discovered data by routes, you associate each discovery interface with a network view. You must have a network view configured for each discovery interface, and you cannot share the same network view with multiple discovery interfaces on the same Probe member. However, discovery interfaces on different Probe members can share the same network view.

To map discovery interfaces to their respective network views, complete the following:

1. From the Grid tab, select the Grid Manager tab, and then click Discovery.
2. In the Services tab, select the check box of the Probe member you want to configure, and then Click Edit -> Member Discovery Properties in the Toolbar.
3. In the Member Discovery Properties editor, select the General tab and complete the following:
   - Discovery Interfaces: Discovery members must have a designated interface or interfaces over which discovery traffic takes place. By default, appliances use the LAN1 port for discovery traffic. You may designate other ports such as the LAN2, MGMT,
and VLAN ports as the discovery interfaces. These ports must first be defined in the member network settings before they can be used for discovery. You cannot modify the discovery interface settings while the discovery service is running on the appliance.

**Note:** The VLAN interfaces you configured on any Network Insight appliances are used for discovery only. Other services are not supported on these appliances for VLANs. For information about how to define network interfaces on the appliance, see Configuring Ethernet Ports.

The Discovery Interfaces table displays all interfaces you have configured on the member. To discover using multiple interfaces, you must associate each interface with an available network view. A single default network view exists in NIOS by default. All networks created or discovered for NIOS management must be part of a network view. If more than one network view exists in the Grid, you can map a network view other than the default view to the interface. This essentially serves to allow one or more discovery members to perform discovery on separate routing domains, because a network view is comprised of a single routing domain with its own networks. If you do not want to use a configured interface as the discovery interface, simply leave the network view empty or unassigned for that interface. When you first set up an interface, no network view is assigned to the interface by default.

The appliance displays the following for each interface you configure on the Probe member. To modify the network view for an interface, click the Network View column and select the network view you want to associate with the corresponding interface.
- **Interface:** Displays the name of the interface. You cannot modify this field. Discovery supports the LAN1, LAN2, MGMT, and VLAN interfaces. You must first define these interfaces for the member before using them for discovery.
- **VLAN Tag:** Displays the VLAN tag or ID for the corresponding VLAN interface. This field is left blank for all physical interfaces. You cannot modify this field.
- **Network View:** Displays the current network view with which the interface is associated. An interface is not associated with any network view and this field is left blank by default, which means the interface is not used as a discovery interface. To modify the network view, click the Network View column for the corresponding interface and select the network view you want to reassign to the interface from the drop-down list. The appliance associates an interface with the default network view if you have not configured additional network views.

4. Save the configuration.

**Configuring Discovery Properties**

To ensure successful discovery, complete the following configurations for the Grid and Grid members that are acting as the Consolidator and Probes before you start a discovery:

- Define the basic polling methods, such as SNMP collection, CLI collection, and others for the Grid. For more information, see **Defining Basic Polling Settings for the Grid**.
- Define advanced polling settings for TCP scanning and Ping sweeps if you have selected these polling methods. You can also select to use DHCP routers as seed routers or log discovery events to the syslog while configuring advanced polling settings. For more information, see **Defining Advanced Polling Settings for the Grid**.
- Configure SNMP and CLI credentials if you have selected SNMP Collection and CLI Collection as the polling methods. For more information, see **Configuring SNMP1/v2 Credentials for Polling**.
- Enable discovery or port configuration blackout periods, as described in **Defining Blackout Periods** and **Defining Port Configuration Blackout Periods**.
- Configure automatic network view mapping for unassigned VRFs that have been discovered, as described in **Configuring Automatic VRF Mapping**.

**Note:** You must be a superuser to configure discovery properties for the Grid. Some settings, such as seed router definition, take place only on Probes.

**Defining Basic Polling Settings for the Grid**

Grid polling settings apply to all Probe members and all discovery networks that are assigned to a Probe. You can override the Grid settings at the Probe member and network levels. Only superusers can modify Grid-wide discovery settings.

To define basic polling settings or to override Grid settings on Probe members and networks, complete the following:

1. For Grid: From the Grid tab-> GridManager tab -> Discovery service, select Edit -> Grid Discovery Properties from the Toolbar.
   - For members: From the Grid tab-> GridManager tab -> Discovery service, select Edit -> Member Discovery Properties from the Toolbar.
   - For networks: From the IPAM tab, select the network check box and click the Edit icon.
2. In the Grid Discovery Properties, Member Discovery Properties, or (IPv4 or IPv6) Network editor, click the Polling tab, and then complete the following in the Basic tab:
   - For Probe members and networks, click Override to override the Grid settings.
   - **SNMPCollection:** Select this to execute SNMP protocols to discover and collect information such as traceroute/path collection, vendor and model, SNMP credential collection, routing and ARP tables, switch port data, and VLAN configuration data. If you disable SNMP collection, previously discovered data remains available for viewing; no new data is added and no existing data is removed. Note that some devices may not support SNMP, and some devices also may not enable SNMP by default.
   - **CLI Collection:** Select this if you expect to use Network Insight to discover devices that support CLI connectivity through Telnet or SSH and that you possess admin account information. NIOS can use device admin account logins to query network devices for discovery data collection, including IP configuration, port configuration, routing and forwarding tables, and much more. You must also provide the command-line credentials information as the credentials in the Grid Discovery Properties editor.
Note: CLI Collection is the default polling method if SNMP is enabled on the member.

- **Port Scanning**: Select this to probe the TCP ports. Ensure that you go to the Advanced tab to configure more settings for this option. Should you disable Port Scanning, NIOS attempts no port probes other than SNMP on any device.
  - **Profile Device**: If enabled, NIOS attempts to identify the network device based on the response characteristics of its TCP stack, and uses this information to determine the device type. In the absence of SNMP access, the Profile Device function is usually the only way to identify non-network devices. If disabled, devices accessible via SNMP are identified correctly; all other devices are assigned a device type of Unknown. Profile Device is disabled by default for network polling.
- **Smart IPv4 Subnet Ping Sweep**: Select this to execute Ping sweeps only on subnetworks that are known to exist but no IPs can be found within the subnet, such as through ARP or other means.
- **Complete Ping Sweep**: Select this to enable brute-force subnet Ping sweeps on IPv4 networks. An ICMP ping is broadcast to all addresses in a subnet. Subnet ping sweeps are used as a last resort in the discovery process. Perform a subnet ping sweep if NIOS cannot identify any network devices in a given subnet.
- **Subnet ping sweeps should be performed no more than once per day, and will stop on a given subnet once NIOS Discovery locates a network device and is able to collect data from it. Ensure that you configure advanced settings for this option in the Advanced tab.

Note: Note: NIOS will not perform Smart Subnet ping sweeps on subnets larger than /22. NIOS also will not perform Ping sweeps on IPv6 networks because of the dramatically greater scale of network addresses in the IPv6 realm. The Complete ping sweep differs from the Smart Subnet ping sweep in the following ways: the Complete ping sweep will run only against the specified range; the sweep will run regardless of the range size, and the sweep will run regardless of the number of discovered devices within the specified range.

- **NetBIOS Scanning**: Select this to enable NIOS to collect the NetBIOS name for endpoint devices in the network. This feature can be enabled only by users with SysAdmin privileges. This feature is globally disabled by default (and also for device groups) to prevent unexpected scanning of the network by a new collector.
- **Automatic ARP Refresh Before Switch Port Polling**: Select this to enable refreshing of ARP caches on switches and switch-routers in the managed network before NIOS performs polling of switch ports. Enabling this feature applies only to switched Ethernet devices. This feature enables more accurate detection of all endpoint devices on L2 switches. Without ARP refresh, some endpoint devices may not be detected. This feature is globally disabled by default. Individual ANPs can also be set to enable or disable this feature.
- **Switch Port Data Collection**: Select this to enable the Probe member to poll L2 enterprise switches. You can completely disable switch port polling by deselecting this check box. You can also separately schedule polling for switch port data collection as follows:
  - **Periodic Polling**: Define regular polling time periods. Choose a polling interval of 30 or more Minutes or in between 1 and 24 Hours.
  - **Scheduled Polling**: Schedule recurrent polling based on hourly, daily, weekly or monthly time periods. Choosing this option, click the Calendar icon and a Polling Schedule editor appears; click the Edit icon to make scheduling changes. Choose a recurrence pattern of Once, Hourly, Daily, Weekly or Monthly; in all cases, you must choose an Execution Time.

3. Save the configuration.

**Defining Advanced Polling Settings for the Grid**

If you have selected any basic polling settings that involve the TCP scanning and Ping sweeps, you must configure additional settings to ensure that these polling methods function properly in a discovery. Advanced SNMP polling settings consist of choosing the TCP Scan Technique, along with a number of specialized settings for Ping Sweeps and other operations.

To defining advanced Grid-wide polling settings for TCP scanning and Ping sweeps, complete the following:

1. For Grid: From the Grid tab -> Grid Manager tab -> Discovery service, select Edit -> Grid Discovery Properties from the Toolbar. For members: From the Grid tab -> Grid Manager tab -> Discovery service, select Edit -> Member Discovery Properties from the Toolbar.
   For networks: From the IPAM tab, select the network check box and click the Edit icon.
2. In the Grid Discovery Properties, Member Discovery Properties, or (IPv4 or IPv6) Network editor, click the Polling tab, and then complete the following in the Advanced tab:
   For Probe members and networks, click Override to override the Grid settings.

   - **TCP Scan Technique**: Select the TCP technique you want to use for the discovery. The default is SYN. For more information, see TCP.
     - **SYN**: Select this to quickly perform scans on thousands of TCP ports per system, never completing connections across any well-known port. SYN packets are sent and the poller waits for a response while continuing to scan other ports. A SYN/ACK response indicates the protocol port is listening while a RST indicates it is not listening. The SYN option presents less impact on the network.
     - **CONNECT**: Select this to scan IPv6 networks. Unlike the SYN option, complete connections are attempted on the scanned system and each successive TCP protocol port being scanned.

   In the port table, select the check boxes of the TCP ports you want to discover. You can select all ports by clicking the check box in the header.
   Optionally, you can click the Add icon and complete the following to add a new port to the list:
     - **Port**: Enter the port number you want to add to the list. You must enter a number between 1 and 65535.
     - **Service**: Enter the name of the service.
3. You can also delete a specific TCP port in the list, or select multiple ports for deletion.

- **Purge expired assets data after**: Removes records of discovered assets that are no longer reachable after a specified period of time. The default is set to one day.
- **Purge expired device data after**: Removes records of discovered network infrastructure devices that are no longer reachable after a specified period of time. The default is set to seven days, a more forgiving value given that devices sometimes require maintenance, upgrades or repairs, or in cases where hosts leave the network on long trips.
- **ARP Aggregate Limit**: Determines the largest ARP table collectible by discovery. The default is set to 30 ARP table entries (MAC Addresses).
- **Route Limit**: Limits the size of the routing table that discovery is required to collect from any given device. Some routers can have tables in the hundreds of thousands of entries, and collecting such a large body of data can impose performance problems in the network and in discovery data collection. This setting defaults to 3000, and automatically excludes BGP routes from collection. Consult Infoblox Technical Support before making changes to this value.
- **Ping Sweep Timeout (ms)**: Period of time allowed, in milliseconds, before Ping times out to any given device. Default is 1000 ms.
- **Ping Sweep Attempts**: The number of attempts on each address in a Ping sweep before the sweep continues.
- **Ping Sweep Frequency**: Defaults to 1, because ping sweep should not be executed more than once a day when the feature is enabled at the grid level or for a given discovery range. This setting affects the Smart Ping Sweep and Complete Ping Sweep features under Grid Discovery Properties.
- **ARP Cache Refresh**: Defines the time period between ARP refreshes by Network Insight across all switch ports. Before any otherswitchport polling and discovery operations take place (including any global discovery polling operations initiated by the administrator), another ARP refresh is carried out by the Probe appliance regardless of the time interval. The default is five minutes, because switch forwarding tables are frequently purged from LAN switching devices. (The default on Cisco switches is five minutes/300 seconds.) Network Insight primarily uses ARP Cache refreshes to improve the accuracy of end-device discovery. Without this feature, some endpoints may not be discovered and cataloged.
- **Ignore Conflict Duration**: Used when resolving conflicts and when choosing the option to Ignore the conflict when resolving it. The length of time during which conflicts is ignored is defined with this setting. Increments can be defined in Hours or Days.
- **Number of discovered unmanaged IP addresses per notification**: The maximum number of unmanaged IP addresses that the appliance discovers before it sends SNMP and email notifications, if enabled. The appliance resets the counter after it hits this number and sends notifications. The default is 20.
- **Interval between notifications for discovered unmanaged IP addresses**: This number determines how often the appliance sends SNMP and email notifications, if enabled, when it discovers the maximum number of unmanaged IP addresses (configured for Number of discovered unmanaged IP addresses per notification). This is the time interval between two notifications for discovered unmanaged objects. Select the time unit from the drop down menu. The default is five minutes.
- **DNS Lookup Option**: Specify whether you want to perform a reverse DNS lookup from discovered IP addresses. Select one of the following from the drop-down list:
  - **Network Devices**: Select this to resolve network device (switches and routers) IP addresses. This option is selected by default.
  - **Network Devices and End Hosts**: Select this to resolve both network device (switches and routers) and end host IP addresses.
  - **Off**: Select this to turn off reverse DNS lookups for discovered IP addresses.
- **DNS Lookup Throttle**: This is the value in a percentage that throttles the traffic on the DNS servers. Setting a lower value reduces the number of requests to DNS servers. You can specify a value between 1 and 100. The default value is 100.
- **Disable discovery for networks not in IPAM**: Enabling this setting disallows Network Insight from executing discovery on any infrastructure networks that are not presented in the Infoblox IPAM system, e.g., present and managed in a network view or network container.
- **Authenticate and poll using SNMPv2c or later only**: For credential discovery and device polling exclusively using SNMPv2c and up, preventing use of SNMPv1, enable this check box.
- **Use DHCP Routers as Seed Routers**: Select this so the Probe members can use the default gateways for associated DHCP ranges and networks as seed routers to more quickly discover and catalogue all devices (such as endpoint hosts, printers and other devices). All such default gateways are automatically leveraged by discovery, and no further configuration is necessary unless you wish to exclude a device from usage.

**Note**: Check for a list of configured DHCP seed routers for any discovery Probe member in the **Seed** tab -> **Advanced** tab of the **Member Discovery Properties** editor.

- **Log IP Discovery events in Syslog**: Sends a message to the configured Syslog service when an IP address of an active host is discovered.
- **Log network discovery events in Syslog**: Sends a message to the configured Syslog service when a network discovery process takes place in the Grid.

4. Save the configuration.

**Configuring SNMP1/v2 Credentials for Polling**

**Note**: You can test SNMPv1/v2c and SNMPv3 credentials against any device or any IP address, at the Grid level or from any Probe member or network view. For more information, see **Configuring SNMPv3 Properties** and **Testing SNMP and CLI Credentials**.
You can test username/password credentials or an Enable password credential. You can also combine a username/password credential and an Enable password credential as part of the same test. A community string similar to a password in that the discovered device accepts queries only from management systems that send the correct community string. Note that this community string must exactly match the value that is entered in the managed system. If you have a substantial list of community strings in this list and need to find a specific string, enter the value in the Go To field and click Go. To remove a community string entry, select the check box and click the Delete icon.

5. Optionally, you can test the credentials you added to the list by selecting a community string check box and clicking Test Credentials, as described in Testing SNMP and CLI Credentials.

6. To export the entire list of community strings in a table file readable by a spreadsheet program, click the Export icon and choose Export Data in Infoblox CSV Import Format. To export all data in a different format, click the Export icon and choose Export Visible Data.

Configuring SNMPv3 Properties

SNMPv3 allows the use of two secret keys for every credential—one for authentication, and another for encryption. Network Insight allows flexible application of keys—authentication but no encryption, for example. You define users in one of three ways:

- SNMPv3 user, with no authentication or privacy credentials
- SNMPv3 user, with authentication but no privacy credentials
- SNMPv3 user, with both authentication and privacy credentials

You can import sets of SNMPv3 credentials from an Infoblox CSV Import format data file.

1. From the Grid tab, select the Grid Manager tab, and then click Discovery.
2. For the Grid: Click Edit -> Grid Discovery Properties in the Toolbar.
   For the Probe member: Select the member check box, and then click Edit -> Member Discovery Properties in the Toolbar.
3. Click the Credentials tab. To override Grid settings for a Probe member, click Override.
4. Click the Add icon to add a new community string entry to the list. Click the Read Community cell and enter a text string that the management system sends together with its queries to the network device during discovery.
   A community string is similar to a password in that the discovered device accepts queries only from management systems that send the correct community string. Note that this community string must exactly match the value that is entered in the managed system. If you have a substantial list of community strings in this list and need to find a specific string, enter the value in the Go To field and click Go. To remove a community string entry, select the check box and click the Delete icon.
5. If you have a substantial list of SNMPv3 entries and need to find a specific entry, enter the value in the Go To field and click Go.
6. To remove an SNMPv3 authentication entry: select the check box and click the Delete icon.
7. To export the entire list of community strings in a table file readable by a spreadsheet program, click the Export icon and choose Export Data in Infoblox CSV Import Format.
   a. To export just the subset of data that is visible in the dialog, click the Export icon and choose Export Visible Data.
   b. A Show Passwords option allows the secret keys to be visible in the import.

Configuring CLI Discovery Properties

SNMP protocols provide a powerful means of querying devices for broad arrays of information. The CLI discovery feature is required for port control tasks including port configuration and network provisioning and de-provisioning, but is not used for other discovery operations or to otherwise manage devices. By default, Probe appliances inherit their member discovery properties, including CLI credential sets, from the Grid level. Enable passwords are entered in separate records and kept as a separate list in Grid Manager.

You manage CLI credentials for devices in similar fashion to SNMP credentials, by defining a global set of Admin account/password tuples (and Enable passwords) at the Grid level; and specifying credentials and Enable passwords for individual devices at the member level, when necessary. Should such a credential not work for a given device, or if command-line access is lost for a device, Network Insight re-guesses credentials from the Grid-level credential list, including vendor defaults if available.

Note: You can test username/password credentials or an Enable password credential. You can also combine a username/password credential and an Enable password credential as part of the same test.

1. From the Grid tab, select the Grid Manager tab, and then click Discovery.
2. For the Grid: Click Edit -> Grid Discovery Properties in the Toolbar.
   For the Probe member: Select a member check box, and then click Edit -> Member Discovery Properties in the Toolbar.
3. Click the Credentials tab -> CLI tab. To override Grid settings for a Probe member, click Override.
4. Click the Add icon to add a new CLI username/password entry to the list. Select the Credential Type, which can be one of two choices:
5. In the Login Credentials list, click the Add icon to add a new CLI username/password entry:
   - Protocol: Select SSH or Telnet. Infoblox recommends the use of SSH.
     • SSH — SSH credentials require both a username and password. The default protocol is SSH.
     • Telnet — In Network Insight, Telnet credentials must use both a username or password.

Note: Should you choose to use a Telnet-based credential, Network Insight requires both the username and password for the login account. This also applies when you override the CLI credentials on objects such as a fixed address, host or IPv4 reservation. For more information, see the section Defining CLI Credentials Settings for Objects.
- **Name** — Username for the CLI login account.
- **Password** — Login password for the CLI login account.
- **Comment** — A text comment describing the CLI login account.
- **Order** — By default, Network Insight inserts the new credential record at the bottom of the credentials list, which is reflected by its Order value, showing the order used for attempting use of CLI credentials. Enter a new value in the Order field if you want the new credential to be in a position other than the last in order.

6. In the **Enable Credentials** list, click the Add icon to add a new Enable password entry:
   - **Protocol** — SSH or Telnet. Infoblox recommends the use of SSH.
   - **Password** — Enable password for device configuration access.
   - **Comment** — A text description.
   - **Order** — By default, Network Insight inserts the new record at the bottom of the list, reflected by its Order value, showing the order used for attempting use of the CLI credentials. Enter a new value in the Order field if you want the new credential to be in a position other than the last in order.

7. Click **Save & Close** to save changes. You may also select **Save** to keep the dialog box open for further changes. You can press Tab to navigate across the fields for the credential entry.

To test CLI credentials for the current appliance, see *Testing SNMP and CLI Credentials*.

### Defining CLI Credentials Settings for Objects

You can override CLI credentials, and enable password credentials, for IPAM objects such as fixed addresses, IP reservations, and host objects. You can also do so for networks under IPAM and DHCP.

When you do so, you define and test the CLI credentials and enable passwords locally to the object.

1. From the **Data Management** tab, select the **IPAM** tab. The IPAM Home page appears.
2. In the IPAM IP List page or the IPAM IP Map page, navigate to the network and then the IP associated with the object you want to edit.
   
   **Note:** For each network, the IP list page provides a **Type** data column showing the IPAM object type that is associated with any IP address. Also check the **MAC Address** column in the IP List page for information about associated objects.

3. Click the IP address. In the IP address page, click the **Related Objects** tab.
4. Select the check box for the object in the Related Objects panel and click **Edit**.
5. In the object editor, click the **Discovery** tab.
6. For the object, click the **Override CLI Credentials** check box to override the inherited set of CLI credentials taken from the Grid level.
   
   By default, CLI credential definitions use SSH at the object level. Select the **Allow Telnet** check box if you want to allow both SSH and Telnet credential usage; Infoblox recommends SSH because of better security.
7. Enter the **Name** and **Password** values, and the **Enable Password** value.
8. Click **Test CLI Credentials** to test the CLI discovery credential settings applied to the object.
9. When finished, click **Save & Close**.

### Testing SNMP and CLI Credentials

After configuring SNMP and CLI credentials, you can click **Test Credentials** in the SNMP Credentials or CLI Credentials panel to test the credentials. Credential testing ensures that the configured credentials work for as many devices and networks as possible. The procedure in this section applies to both the Grid and the member levels. You can override the Grid settings at the member level.

For CLI credentials, you can test an admin login name and password tuple as well as a following enable credential, if necessary. You can also override CLI credentials and enable credentials for IPAM objects such as fixed addresses, IP reservations, and host objects. You can test any credential set, an enable credential or both in combination against any device within any network view. Network Insight sets the login sequence to match the command-line standards for the selected device.

To test SNMP credentials or CLI credentials, complete the following:

1. From the **Grid** tab, select the **Grid Manager** tab, and then click **Discovery**.
2. For the Grid: Click **Edit** -> **Grid Discovery Properties** in the Toolbar.
   
   For a Probe member: Select a **member** check box, and then click **Edit** -> **Member Discovery Properties** in the Toolbar.
3. In the **Grid Discovery Properties** or **Member Discovery Properties** editor, click the **Credentials** tab -> **SNMPv1/v2** tab, **SNMPv3** tab, or **CLI** tab.
4. Select the check box or check boxes for the credentials and/or enable credentials (if applicable) you want to test. For a Probe member, click **Override**, and then select the credential check boxes.
5. Click **Test Credentials**.
6. In the **Test SNMP Credentials** editor, complete the following:
   - **IP Address**: Select this to test the credential against an IP address of a reachable device in a network (even if it has not been discovered or managed through NIOS) within a specified network view. Enter the IP address in the field. Ensure that you select the respective network view in which this IP address resides.
   - **Network View**: If you have multiple network views, select the network view in which the IP address resides from the drop-down list. If you have only one network view, which is the default view, the Network View drop-down list is hidden by default. NIOS conducts credential testing for the IP address in the selected network view.
   - **Device**: Select this to test against a selected device. Click **Select Device** and the **Device Selector** appears. If you have multiple
network views, you must first select the network view in which the device resides from the **Network View** drop-down list, located at the upper left-hand corner of the selector. If you have only one network view, which is the default view, the **Network View** drop-down list is hidden by default. You can check the device categories under **All Devices** to locate discovered switches and routers or any unmanaged devices previously detected by discovery under NIOS. You can explore categories including Discovered Switches/Routers, Microsoft Windows Devices (this can include items such as Windows Servers of various types), Router and Wireless Access Point Devices, Unmanaged, and others. By default, all devices previously discovered appear in this selector. If you have a long list of devices, you can enter a device name search value or a search expression in the **Find** field and click **Go**. You can also click **Show Filter** to narrow down your selection by selecting available filters. Click **OK** after you have selected a device and its corresponding network view.

7. Click **Start** to begin testing the credential against the IP address or selected device. The communication and testing processes appear in the lower pane of the editor.

**Note:** If the specified IP address is excluded from all discovery ranges or is not part of the selected network view, or the credential is entered with missing information, a message appears at the top of the editor after clicking **Start**. Otherwise, the test begins and its process and results appear in the lower pane of the editor.

### Defining Seed Routers for Probe Members

Seed routers can be defined only on Probe appliances. You can define seed routers that NIOS uses in quickly performing network discovery. Definition of seed routers is highly recommended for IPv4 networks and is required for IPv6 networks. For the discovery of any IPv6 networks, you must use seed router values comprised of at least one well-connected IPv6 router, preferably with routes to all other networks to be managed. In some cases, seed routers may not have the full routing tables or be unable to provide full information for some reason. The general rule of thumb is that more seed routers are better, but the connectivity of seed router(s) also helps determine how many seed routers you need. Avoid having more seed entries than necessary.

You must associate each seed router with a network view so the appliance can properly discover virtual networks when using multiple seed routers.

**Note:** All NIOS Probe members automatically use their default gateway as a seed router. These gateways are automatically displayed in the table. For effective use of seed routers, you must also provide SNMP credentials to NIOS to allow it to pull the key routing and connectivity information, including the IPv6 routing table and the local Neighbor Discovery Cache, from the device. If you do not define a seed router, it is recommended that you enable discovery for a network or DHCP range.

You can check **Discovery Status** to see whether a seed router is successfully being reached and whether the seed is providing information. By reviewing discovery status for each seed router, you can determine whether Network Insight should be able to discover the network successfully, or if there are possible configuration errors preventing network discovery, without having to wait to see what Network Insight finds. For seed routers, **Reached Status** and **Overall Status** should both read **Passed**.

To add, view, or delete seed routers for a Probe, complete the following:

1. From the **Grid** tab, select the **Grid Manager** tab, and click **Discovery**.
2. Select the check box for any Probe appliance on the Discovery page and click **Edit -> Member Discovery Properties** from the Toolbar.
3. In the Member Discovery Properties editor, Click the **Seed** tab. Grid Manager displays the following:
   - Click the Add icon to add a seed router. Grid Manager adds a row to the table. Complete the following in the table:
     - **Router:** Click this field and enter the IP address for the desired IPv4 or IPv6 seed router. Note that you can assign a seed IP address to different network views if your deployment has overlapping IP addresses.
     - **Network View:** Displays the current network view with which the interface is associated. A newly added seed IP does not have any associated network view by default. From the drop-down list, select the network view you want to reassign to the interface.
     - **Comment:** Enter information about the seed router.

You can delete a seed router by selecting it and then click the Delete icon. Note that you cannot delete any seed router that is a default gateway.

### IPv6 Seed Router Usage

For the discovery of any IPv6 network, you must use seed router values, comprised of at least one well-connected IPv6 router, preferably with routes to all other networks to be managed. In some cases, seed routers may not have the full routing tables or be unable to provide full information for some reason. The general rule of thumb is that more seed routers are better, but the connectivity of seed router(s) also helps determine how many seed routers you need. Avoid having more seed router entries than necessary.

**Note:** For effective use of seed routers, provide SNMP credentials to the Probe member to allow it to pull the key routing and connectivity information, including the IPv6 routing table and the local Neighbor Discovery Cache, from the device. For more information, see [Defining Seed Routers for Probe Members](#).

### Configuring Cisco Application Policy Infrastructure Controller (APIC)

Integrating Cisco APIC on NIOS provides visibility into your Cisco APIC infrastructure, which allows you to view and manage discovered IP addresses from Cisco ACI cluster. You can discover the SDN Controller and Elements (Spine, Leaf, End Points) using the Network Insight...
To configure Cisco APIC on NIOS, complete the following:

1. From the Grid tab, select the Grid Manager tab, and then click Discovery.
2. Select the member check box, and then click Edit -> Member Discovery Properties in the Toolbar.
3. Click the Cisco APIC Configuration tab and click the Add icon and complete the following:
   - **Protocol**: Select HTTP or HTTPS as the protocol. When you select HTTPS, you must upload the corresponding SSL CA certificate to the Grid in order for NIOS to communicate with Cisco APIC, as described in Managing Certificates.
   - **Network View**: Select the network view to which the device is associated.
   - **Username**: The login name of Cisco APIC.
   - **Password**: The login password of Cisco APIC.
   - **Address**: Enter the hostname or IP address of Cisco APIC.
   - **Comment**: Enter additional information Cisco APIC.
4. Click Add to add Cisco APIC.
5. When finished, click Save & Close.

### Configuring Automatic VRF Mapping

You can configure Network Insight to automatically assign network views to VRFs by defining mapping rules that match unassigned VRFs—VRFs that do not have associated network views. You can also disable the automatic VRF mapping and manually assign network views to discovered VRFs, as described in Viewing Discovered VRFs and Mapping Network Views.

When you enable automatic VRF mapping, you can add VRF mapping rules that Network Insight uses to map network views to VRFs that do not already have an assigned network view. When you configure mapping rules, you can define criteria using regular expressions and place the rules in specific order to define their priorities. Network Insight matches the rule criteria to the discovered VRF names, starting with the first rule in the VRF Mapping Rules table. You also have a choice to map an unassigned VRF to the network view from which one of the interfaces the VRF is reached, if none of the mapping rules match the VRF name.

To configure automatic VRF mapping and mapping rules for unassigned VRFs, complete the following:

1. From the Grid tab, select the Grid Manager tab, and then click the Discovery service.
2. In the Grid Discovery Properties editor, select the VRF Mapping Rules tab, and then complete the following:
   - **Enable the automatic VRF mapping rules defined below for unassigned VRFs**: Select this to enable automatic VRF mapping so you can define mapping rules that Network Insight uses to map network views to unassigned VRFs that match the criteria of the rules.
   - **Enable the automatic VRF mapping rules and system mapping extensions**: Select this to enable the VRF Mapping Rules table so you can define mapping rules that Network Insight uses to map network views to unassigned VRFs that match the criteria of the rules; and in cases where none of the rules match a VRF name, Network Insight maps the VRF to the network view from which one of the interfaces the unassigned VRF is reached.
   - **Disable automatic VRF mapping and only use manually defined VRF mapping**: Select this to disable the VRF Mapping Rules table. When you select this, Network Insight does not perform any evaluation of the VRF mapping rules. You can manually assign or unassign network views to the discovered VRFs, as described in Viewing Discovered VRFs and Mapping Network Views.

When you enable automatic VRF mapping, you can add mapping rules to the VRF Mapping Rules table, as follows:

1. Click the Add icon, and the appliance adds a row to the table.
2. In the table, click each of the following fields and enter the values accordingly:
   - **Network View**: The network view that you want to use for all matching VRFs. You can click this field and select a network view from the drop-down list that displays all the configured network views, including the default network view.
   - **Order**: The order and priority in which Network Insight evaluates the mapping rules. Each time you add a new rule, the appliance automatically appends the rule to the end of the list and assigns the next incremental number to the rule. To reorder the list, you can select a rule and use the up and down arrows next to the table to move the rules to its desired position so you can set the priority for the rule evaluation. Network Insight evaluates the rules based on the order, starting with 1 as the highest priority.
   - **Criteria**: The criteria that Network Insight uses to match the VRF name of an unassigned VRF. You can use POSIX regular expressions to define the mapping criteria. The appliance validates the rule when you save the configuration, and it returns an error message if the criteria is invalid. For more information about regular expressions, see Regular Expressions.
   - **Comment**: Enter a comment about the VRF mapping rule. Click the Add icon again to define another mapping rule.
3. Save the configuration.

**Note**: All the VRF mapping rules that are currently configured for the Grid are displayed in the VRF Mapping Rules table.

You can also do the following in the VRF Mapping Rules tab:

- Select a specific rule and click the Delete icon to remove it from the table.
- Use the up and down arrows next to the rules table to reorder the rules.
- Use the Go to function to search for a specific mapping rule. With the autocomplete feature, you can just enter the first few characters of a network view in the Go to field and select the network view from the possible matches.

### Excluding IP Addresses from Discovery
**Note:** You use the IPv4 Network or IPv6 Network editors to exclude IP addresses or ranges of IP addresses from discovery within the specified network. For more information, see [Disabling Discovery for a Network](#).

Host records, fixed address and IPv4 reservations can be excluded from discovery. You may also exclude an IP address or a range of IPs within a network from discovery.

**Note:** You may create a network and choose not to discover it at that time, by disabling both [Enable Immediate Discovery](#) and [Enable Discovery](#). If you disable the [Enable Discovery](#) check box, the network will never be discovered unless you change the setting again at a later time. Conversely, you can explicitly exclude specific IPs or IP ranges from discovery. Discovery will never take place on these IPs unless the admin specifically changes their exclusion setting.

Administrators can specify IPv4 and/or IPv6 addresses that must be immediately discovered by the appliance. Some devices may need exclusion because they do not support SNMP, or for other organizational reasons. Devices matching IP addresses selected for immediate discovery (using the [Discover Now](#) feature described in [Using Discover Now to Discover an Existing Object](#)) are given one-time priority over other discovered devices, for data collection and counting toward any device found matching the license limits. A device specified through an IP address can also be excluded from discovery or management.

### Quick Exclusion of IPs from Discovery

You can use the IPAM IP Map or IP List page to quickly exclude IP addresses and selected ranges of IP addresses from discovery. For example, you may have Infoblox appliances or routers that provide the gateway to networks that are already managed by Grid Manager, or devices on which you do not wish to have discovery operations take place.

1. From the **Data Management** tab, select the **IPAM** tab. The IPAM Home page appears.
2. Click on any network or network container in the list. The **IP Map** appears for the selected network.

**Note:** You may also use the **List** page for the selected network to exclude IPs or selected ranges of IPs. However, you have to page through or search through the pages comprising the list view to locate the IPs you want to exclude. (If you know the IP address value in the **List** view but it does not appear on the page, enter it in the **Go to** field to search for the IP.) The **IP Map** view allows you to view every IP address in a selected network, such as a /24 prefix.

3. Select one or more IPs in the map. **SHIFT+click** to select a series of contiguous IPs. **CTRL+click** to select non-contiguous IPs.
4. Expand the Toolbar and click **Exclusion** \(\rightarrow\) **Enable Exclusion**. The selected IP addresses are excluded from any discovery actions.

**Note:** You can click the **Action icon** 


for any List record and choose **Exclusion** \(\rightarrow\) **Enable Exclusion**.

To locate an IP to exclude within a network container:

1. From the **Data Management** tab, select the **IPAM** tab. The IPAM Home page appears.
2. Select the network container by clicking it. The IPAM Home page changes to display the List page, showing the list of networks within the container.
3. Click the network that has the IP in its space that you wish to exclude.
4. Select the network IP address from the **List** table. If you know the IP address value but it does not appear on the page, enter it in the **Go to** field to search for the IP.
5. Expand the Toolbar and choose **Exclusion** \(\rightarrow\) **Enable Exclusion**.

A parent network container may exclude IPs, and you may add and remove discovery exclusions within network containers. You can drill down to the child networks in the **Net Map** view to perform exclusions on IPs. For example, consider a /16 network container that has a number of smaller /24 child networks within it. Right-clicking on any child network in the network container and choosing **Edit** from the popup menu, opens the editor with its **Discovery Exclusions** tab, where you can perform exclusions within the child network.

### Creating a New IPAM Object and Excluding it from Discovery

You can create a new object from the main **Data Management** \(\rightarrow\) **IPAM** or **Data Management** \(\rightarrow\) **DHCP** pages.

1. From the **Data Management** tab, select the **IPAM** or **DHCP** tab.
   a. For IPAM, the **IPAM** home page appears, listing all networks reachable by IPAM.
   b. For DHCP, the home **Networks** page appears, showing all networks reachable by DHCP.

**Note:** The network lists between IPAM and DHCP will likely differ, because networks can be set to be Disabled from DHCP. IPAM provides a complete list of all networks configured or discovered by Grid Manager.

2. Select a network from the IPAM home page: by checking the network's check box, searching for the network in the **Go To** box, or using the
Discovering Devices and Networks

To start discovery on connected networks, complete the following:

1. Ensure that your appliances are licensed for discovery.
2. Add the needed seed routers to each Probe appliance, as described in Defining Seed Routers for Probe Members.
3. Add the necessary SNMPv1/v2 and SNMPv3 credentials at the Grid level and/or Member/Probe level. For information, see Configuring SNMPv1/v2 Credentials for Polling, Configuring SNMPv3 Properties, Defining Seed Routers for Probe Members, and Defining Seed Routers for Probe Members.
4. If necessary, add CLI Credentials, including device admin username/password tuples and Enable passwords, at the Grid level and/or Member/Probe level, as described in Configuring CLI Discovery Properties and Testing SNMP and CLI Credentials.
5. If necessary, enable the use of DHCP routers and servers as seeds to increase device discovery, as described in Configuring SNMPv1/v2 Credentials for Polling.

Excluding IP Addresses in Grid Manager

You may exclude IP addresses from discovery from within a number of different contexts in Grid Manager. Under IPAM, you can exclude in the IP Map and IP List pages. The IP List page provides an Exclude data column that directly shows the exclusion status for all IPs in the selected network. Various objects, such as host records, IPv4 and IPv6 fixed addresses, and IPv4 reservations, may be excluded from discovery. You may view excluded IP addresses in the IP List page or in the network editor's Exclusions tab.
6. If you have extensive end host Ethernet segments connected to Ethernet switches, enable switch port discovery, as described in Defining Seed Routers for Probe Members.

With these settings, the Probe appliances automatically begin discovering network infrastructure devices.

You can elect to immediately discover or schedule discovery of new objects that you create and enable under IPAM or DHCP. Objects that allow immediate discovery include the following:

- **IPv4 Fixed Address** (see Configuring IPv4 Fixed Addresses for the complete procedure).
  * You can Enable Immediate Discovery or Exclude from Network Discovery after creating the IPv4 fixed address, and override the SNMP credentials if necessary.
- **IPv6 Fixed Address** (see Configuring IPv6 Fixed Addresses for the complete procedure).
  * You can Enable Immediate Discovery or Exclude from Network Discovery after creating the fixed address, and override the SNMP credentials if necessary.
- **IPv4 Reservation** (see Configuring IPv4 Reservations for the complete procedure).
  * You can Enable Immediate Discovery or Exclude from Network Discovery after creating the IPv4 reservation, and override the SNMP credentials if necessary.
- **Host** (see Adding Host Records for the complete procedure).
  * You can Enable Immediate Discovery or Exclude from Network Discovery after creating the host, and override the SNMP credentials if necessary.
- **IPv4 Network** (see Configuring IPv4 Networks for the complete procedure).
  * You can Enable Immediate Discovery (option is enabled by default) and override inherited discovery Polling Options for the new network.
- **IPv6 Network** (see Configuring IPv6 Networks for the complete procedure).
  * You can Enable Immediate Discovery (option is enabled by default) and override inherited discovery Polling Options for the new network.
- **IPv4 DHCP Range** (see Configuring IPv4 Address Ranges for the complete procedure).
  * You can Enable Immediate Discovery (option is enabled by default) and override inherited discovery Polling Options for the new IPv4 DHCP range.
- **IPv6 DHCP Range** (see Configuring IPv6 Address Ranges for the complete procedure).
  * You can Enable Immediate Discovery (option is enabled by default) and override inherited discovery Polling Options for the new IPv6 address range.

During configuration, you can choose to Exclude from Network Discovery if you wish to postpone discovery for specific object types.

**Note:** Individual IP addresses within a network, and specific object types (IPv4 reservation, fixed address, and host), may be excluded from discovery. You must explicitly select Enable Discovery for other object types (IPv4 and IPv6 Ranges, IPv4 and IPv6 Networks); you can optionally Enable Immediate Discovery.

If you choose not to perform immediate discovery, but do Enable Discovery, the new network or other object is discovered at a normal time determined by Network Insight.

You can manually perform discovery on any object at any time by selecting the object and choosing

Discover Now from the Toolbar. For more information, see Object. When you do so, you see a status icon appear in the Discover Now data column for the object under IPAM, in the Data Management ➔ DHCP page and other locations.

By default, Grid discovery settings are the prevailing settings for all newly created objects. You can override basic discovery polling options for networks and DHCP ranges allowing immediate discovery.

In such cases, local settings take priority. Credentials cannot be overridden for networks and DHCP ranges.

**Using Discover Now to Discover an Existing Object**

**Note:** If after you select a a network, object or IP and the Discover Now button is not enabled, make sure the network or other object has a discovery Probe member assigned to it.

After you create any supported IPAM object, you may wish to perform discovery on it at a later time. You can simply select the object and discover it.

1. From the Data Management tab, select the IPAM tab. The IPAM Home page appears.
2. Select the network or other object over which you want to perform discovery.
   * Depending on the object type, navigate from the network level to the individual IP table in the List page to locate the object for immediate discovery.
3. Expand the Toolbar and click Discover Now.
   * You can also click the Action icon
for the network and choose Discover Now from the menu.

The Probe member associated with the network or other object initiates a discovery procedure.

### Smart Folders and Discovered Devices

Grid Manager maintains a Smart Folder titled Discovered Switches/Routers, under which appears a list of all routers, switches and switch-routers that thus far have been discovered and catalogued through discovery. Clicking a device name opens the device’s main page, with Interfaces, Networks, IP Addresses, Assets and Components panels. For more information, see Managing Discovered Data. Open the Smart Folders category under the Finder menu and click on the Discovered Switches/Routers folder. Clicking on a device name opens the device page under Data Management -> Devices and shows the Interfaces page for the chosen device. For related information, go to Predefined Smart Folders.

### Using the Device Selector

You use a dedicated Device Selector window to choose a discovered device for creating a port reservation with various IPAM objects such as IPv4 reservations, fixed addresses, host records, and provisioning of IPv4 and IPv6 networks on device interfaces; testing SNMP or CLI credentials, and other purposes, as shown in Figure 15.3. Figure 15.3 Using the Device Selector Window

The chosen device is discovered and listed in the Devices panel in IPAM, or any other device on the network under the All Devices category in the left pane of the device selector. Clicking a managed device’s device name selects the device and brings you back to the originating page. Otherwise, select a device and click OK to continue. If you have a long list of devices even after selecting a smart folder, enter a device name search value or a search expression in the Find field and click Go.

### Tips for Quick Navigation

To locate interface and device information quickly, along with associated IPAM objects that may be associated with elements such as port reservations, you can use Device and Interface terms in Global Search. (For additional information on Global Search, see Global Search.) Smart Folders provide another means of locating items such as IP addresses and IPAM objects of various types. Smart Folders provides additional filters for Device Type, Vendor, Model and Version. In a Smart Folder containing interfaces, you can filter by Admin Status, Operation Status, Trunk Status, VLAN ID or VLAN Name, and Description.
Using Smart Folders, you can also isolate all objects of a certain type by creating a smart folder with settings such as: **Type equals IPv4 Fixed Address**. Title the smart folder appropriately, to make clear what data set it is presenting.

### Managing Discovered Data

After a discovery, key information is collected and displayed in the following tabs: **Data Management tab -> Devices -> Interfaces, Networks, IP Addresses**, and **Assets** tabs of Grid Manager. You can view information about each discovered entity in one of these tabs. For more information, see [Viewing Discovered Devices and their Properties](#).

A discovered entity is considered "unmanaged" if it is discovered in a network for which no information is being stored in the NIOS database. You are not able to configure unmanaged objects in NIOS. Depending on the nature of the discovered entity, you may convert certain unmanaged entities into managed objects so you can manage them through Grid Manager. When an entity is in the managed state, you can configure settings such as applying permissions to it, limiting who can modify the configurations and deployments, and when those changes can be applied. You cannot do so with unmanaged objects.

Grid Manager allows you to convert certain unmanaged devices, interfaces, networks, and assets to the following IPAM object types:

- Host record, as described in [About Host Records](#).
- A and PTR records, as described in [Managing A Records](#) and in [Managing PTR Records](#).
- Fixed IPv4 Address, as described in [Configuring IPv4 Fixed Addresses](#).
- Fixed IPv6 Address, [Configuring IPv6 Fixed Addresses](#).

When converting unmanaged entities to managed objects in NIOS, you can choose to convert them one at a time or as a group. To convert a single entity, just select a specific entity and perform the conversion. To convert multiple entities to the same IPAM object type, you can select the entities you want to manage and then perform a bulk conversion. You can also perform an automatic conversion for unmanaged entities in a network view by configuring conversion rules at the Grid level. For information about how to create conversion rules, see [Configuring Automatic Conversion Rules](#).

**Note:** In a bulk conversion, if one or more of the selected entities are not eligible for conversion because they do not have a discovered name (FQDN) or due to other reasons, Grid Manager displays a warning message indicating only eligible entities are displayed in the conversion wizard and qualified for conversion. Those that cannot be converted are ignored and will remain in unmanaged state.

For more information about how to convert unmanaged entities to managed objects, see the following sections:

- For unmanaged devices, see [Converting Unmanaged Devices to Managed Devices](#).
- For unmanaged interfaces, see [Converting Unmanaged Interfaces to Managed Status](#).
- For unmanaged networks from the **Data Management** tab -> **Devices** -> **Networks** tab, see [Converting Unmanaged Networks to Managed Status](#).
- For unmanaged networks from the **IPAM** or **DHCP** tab, see [Converting Unmanaged Networks under IPAM to Managed Status](#).
- For unmanaged IP Addresses, see [Converting Unmanaged IP Addresses to Managed Status](#).
- For unmanaged assets, see [Converting Unmanaged Assets to Managed Status](#).
- For automatic conversions using global conversion rules, see [About Automatic Conversion Rules](#).

### Converting Unmanaged Devices to Managed Devices

**Note:** For convenience, the home [Data Management -> Devices](#) page provides a quick filter to list only managed devices. In the Devices page, all devices highlighted in yellow indicate a device that is unmanaged.

Device discovery allows you to define a fully managed state for any discovered routers, switches, firewalls, end hosts, and other network infrastructure devices. The process differs from converting an unmanaged network, because you can bind a discovered device to a fixed address, a PTR Record, a host record or an IPv4 reservation. Doing so offers the following benefits:

- **Host Record** – Infoblox hosts are data objects that contain DNS, DHCP, and IPAM data of the assigned addresses. Host objects allow you to assign multiple IPv4 and IPv6 addresses to a host. When you create a host record, you are specifying the name-to-address and address-to-name mappings for the IP address that you assign to the host. The Infoblox DNS server then uses this data to respond to DNS queries for the host. This establishes the identity of any infrastructure device or asset on the network. For more information, see [About Host Records](#).
- **A Record** – An A (address) record is a DNS resource record that maps a domain name to an IP address. A records essentially tell DNS that a host exists inside a domain, as part of a forward-mapping zone. All traffic to a domain or subdomain is directed to the IP address specified by the A record. The DNS zone must exist in the Grid Manager before attempting to assign A records to devices. For more information about A records, see [Managing A Records](#).
- **PTR Record** – Maps a device IP address to a host name in a reverse-mapping zone. The zone must already be defined before assigning the new PTR record object. For more information about PTR records, see [Managing PTR Records](#).
- **Fixed Address** – A fixed address represents a persistent link between an IP address and one of the following: MAC address, Client identifier, or Circuit ID/remote ID in the DHCP relay agent option (option 82). Most applications in the current context are for a MAC address. You can configure fixed addresses for network devices, such as routers and printers, that do not frequently move from network to network. By creating fixed addresses for network devices, clients can reliably reach them by their domain names. Some network devices, such as web or FTP servers, can benefit from having fixed addresses for this reason. For more information about these object types, see [Configuring IPv4 Fixed Addresses](#) and [Configuring IPv6 Fixed Addresses](#).

Each object type has its own characteristics that you may apply to specific types of discovered devices. For many infrastructure devices such as
To convert unmanaged devices to managed objects:

1. From the **Data Management** tab, select the **Devices** tab.
2. Click the **Next Page** and **Last Page** icons to locate the device you want to convert.
3. To **convert a single device**:
   - Click the Action icon next to the device you want to convert (this automatically selects it), and then select **Convert → To Host, To A Record, To PTR Record**, or **To Fixed Address** from the menu.
   - To **convert multiple devices (bulk conversion)**: Select the check boxes of the devices you want to convert to the same IPAM object type.
   - From the Toolbar, select **Convert → To Host, To A & PTR Record**, or **To Fixed Address** from the menu.
4. **For a single device**: The respective object editor appears based on the conversion type you have selected. For example, if you select **To Host**, the **Host** editor appears. In the editor, define the required **General** settings for the new object. You can also define other settings you need from any of the tabs in the editor. For details about how to configure these settings, refer to the online Help in Grid Manager or see the appropriate sections in this guide.
   - **For bulk conversion**: The respective bulk conversion wizard (such as the **Convert Unmanaged IP Addresses to Host Record wizard**) appears based on the conversion type you have selected.

**Note**: Network Insight creates the names of the new managed objects using the Discovered Name (FQDN) for the entities being converted. In the wizard, Grid Manager displays the IP addresses of the selected devices that are eligible for conversion in the **Selected IP Addresses** table. Entities that are not eligible for conversion will not be converted and will not appear in this table.

Based on the selected conversion type, complete the following to start a bulk conversion:

- **To Host**: You can select **Enable in DNS** and/or **Enable in DHCP** so the appliance can serve DNS and/or DHCP for the selected IP addresses in the host record. When you enable DNS, you must select a DNS zone for all entities that do not have an FQDN.
- **To A & PTR Record**: Network Insight converts the selected entities to A & PTR records simultaneously. You must select a DNS...
c. **To Fixed Address:** Network Insight automatically converts all selected IP addresses to fixed addresses in a bulk conversion. As with host record and A/PTR record conversions, entities without a Discovered Name are not eligible for conversions to fixed addresses.

In all bulk conversions, you can define extensible attributes for the selected IP addresses. After you configure the necessary settings, you can convert the discovered entities immediately or schedule the conversion by selecting **Later** and entering the date and time.

6. Click **Save & Close** to make the conversion. You can return to the managed object at any time to make further configuration changes.

In the **Managed** column for all converted entities, Grid Manager displays **Yes** to indicate their managed status. You can now manage these IPAM objects through Grid Manager.

### Converting Unmanaged Interfaces to Managed Status

**Note:** For convenience, a device Interfaces panel provides a quick filter to list only managed interfaces for the device. When a device is converted to managed status, interfaces in the device may remain in unmanaged state. If the interface has an IP address that is recognized under IPAM, it may be converted to managed state.

Interfaces that appear in the Interfaces table for a device may be converted to managed status, under specific circumstances. If an interface is bound to an IP address that is present in an IPAM network (for example, a leaf network inside a network container under IPAM), that interface can be converted to managed status.

For any device, any interface with a hotlink to IPAM may be converted. Examples are shown in **Figure 15.5.**

In **Figure 15.5**, two interfaces provide a link to their respective IPAM interface pages, and show an **IPAM Type** of **Unmanaged**. These ports may be converted to IPAM objects and managed under Grid Manager.

1. From the **Data Management** tab, select the **Devices** tab.
2. Click the **Next Page** and **Last Page** icons to locate the device through which you want to locate the interfaces to convert.
3. Click the **Name** link of the device.
4. Click the **Interfaces** tab for the chosen device. This tab lists all ports discovered on the device.
5. To convert a single interface: Click the **Action** icon next to the interface you want to convert (this automatically selects it), and then select **Convert** → **To Host, To A Record, To PTR Record**, or **To Fixed Address** from the menu.

To convert multiple interfaces (bulk conversion): Select the check boxes of the interfaces you want to convert. From the toolbar, select **Convert** → **To Host, To A & PTR Record, or To Fixed Address** from the menu.

6. **For a single interface:** The respective object editor appears based on the conversion type you have selected. For example, if you select **To Host**, the **Host** editor appears. In the editor, define the required **General** settings for the new object. You can also define other settings you need from any of the tabs in the editor. For details about how to configure these settings, refer to the online Help in Grid Manager or see the appropriate chapters in this guide.

**For bulk conversion:** The respective bulk conversion wizard (such as the **Convert Unmanaged IP Addresses to Host Record** wizard) appears based on the conversion type you have selected.

**Note:** Network Insight creates the names of the new managed objects using the Discovered Name (FQDN) for the entities being converted. In the wizard, Grid Manager displays the IP addresses of the selected devices that are eligible for conversion in the **Selected**
Converting Unmanaged Networks to Managed Status

**Note:** When you convert a network to managed status, Grid Manager uses the discovered Router IP for the network to automatically populate the Router IP value in DHCP configurations for the selected network. Conversion for DHCP is optional; you can choose to **Disable DHCP** when you convert the network.

Unmanaged networks listed under discovered devices present the same conversion features as networks listed under IPAM (see the following section **Converting Unmanaged Networks under IPAM to Managed Status**). Begin by examining the **Data Management -> Devices** page, click a discovered device name's Action icon 🔄

and click the device name hotlink. Open the **Networks** tab. The **Managed** column shows one of three possible states for all discovered networks on each device:

- Blank value—indicates that the network is not known to IPAM, because insufficient information is available to identify and catalog the network at the present time, or because the network listed at the device level is for a loopback interface, a disconnected network, or a network prefix that is overlapped by a larger network encompassing that prefix and defined in IPAM. These are also called non-NIOS networks. At the device level, non-NIOS networks are highlighted in light grey;
- **No**—Shows that the network is **not** managed under IPAM/Grid Manager, but enough information is catalogued that the network can be converted to Managed state. This state is required before a network can be converted to managed status. Networks in this state are highlighted in yellow.
- **Yes**—The network is currently managed under IPAM, converted to an IPAM network. At the device level, managed networks are highlighted in white.

Converting a network in the device context is the same as converting it at the top IPAM level. You cannot apply services or IPAM objects to IP addresses in unmanaged networks until the networks are converted to managed status. Many operations cannot be carried out on unmanaged networks, including editing, splitting, resizing, permissions changes and many other tasks.

1. From the **Data Management** tab, select the **Devices** tab.
2. Click the **Next Page** and **Last Page** icons to locate the device through which you want to locate the assets to convert.
3. Click the **Name** of the device.
4. Click the **Networks** tab for the selected device.
5. To convert a single network: Click the Action icon 🔄 next to the network you want to convert to the Managed state (this automatically selects it), and then select **Convert** from the menu.

To convert multiple networks (bulk conversion): Select the check boxes of the networks you want to convert to the Managed state. From the Toolbar, select **Convert** from the menu.

6. The Network editor appears. In the editor, define the required **General** settings for the network. You can also define other settings you need from any of the tabs in the editor. For details about how to configure these settings, refer to the online Help in Grid Manager.

**Note:** Networks inherit discovery setting from their parent networks. Discovery will be disabled for networks that do not have a parent network.

a. If necessary, select the **Disable for DHCP** check box to disallow the converted network from being usable under DHCP.

b. If necessary, click the **Discovery** tab and click **Enable Discovery** to start discovery on the network after it is converted to Managed state. You can also elect not to discover the network, by leaving the check box clear.
Converting Unmanaged Networks under IPAM to Managed Status

**Note:** When you convert a network to managed status, Grid Manager uses the discovered Router IP for the network to automatically populate the Router IP value in DHCP configurations for the selected network. Conversion for DHCP is optional; you can choose to Disable for DHCP when you convert the network.

The IPAM tab lists all discovered networks as unmanaged, highlighted in yellow. Administrators cannot apply services or IPAM objects to IP addresses in unmanaged networks until the networks are converted to managed status. You can explore unmanaged networks through the IP Map and IP List views, but many operations cannot be carried out on unmanaged networks, including editing, splitting, resizing, permissions changes and other tasks.

**Note:** Unmanaged IP addresses that are part of an unmanaged network cannot be independently converted to a managed IP address.

Unmanaged networks can be converted at the IPAM main page and at the device level under Data Management → Devices, selecting a device and opening the Networks page.

Under IPAM, the Managed column for the Network tables can show one of two possible states for all discovered IPAM networks:

- **No**—Shows that the network is not managed under IPAM/Grid Manager, but enough information is catalogued that the device can be converted to Managed state. This state is required before a network can be converted to managed status.
- **Yes**—The network shown in the table is now Managed under IPAM, converted to an IPAM network.

You can discover the network again after it is converted, keep discovery disabled and execute it at another time, or impose blackout periods that limit the time windows under which discovery can execute on the network. Other management benefits include the ability to enable Infoblox services to the network;

1. From the Data Management tab, select the IPAM tab.
2. **To convert a single network:** Click the Action icon next to the network you want to convert to the Managed state (this automatically selects it), and then select Convert from the menu.
   - **To convert multiple networks (bulk conversion):** Select the check boxes of the networks you want to convert to the Managed state. From the Toolbar, select Convert from the menu.
   - You do not need to take further action other than Save & Close to set the network as Managed.
3. If necessary, you can select the converted network and do the following in the Network editor:
4. Select the Disable for DHCP check box to disallow the converted network from being usable under DHCP.
   - If necessary, click the Discovery tab and click Enable Discovery to start discovery on the network immediately after it is converted to Managed state. You can also elect not to discover the network, by leaving the check box clear.
   - **Click Select Member** to choose the Probe member through which the network may be discovered.
   - **Click Select Member** to choose the Probe member through which the network may be discovered.
   - If necessary, click Override under Polling Options, and modify the device discovery polling options for the network. You can also specify Discovery Exclusions, port control settings, or a Discovery Blackout period.
   - A number of associated DNS and DHCP services are also available for configuration for the new IPAM network, including DHCP Forwarding, IPv4 DDNS settings, and an array of other DDI service settings for the network. None of these configurations are required in order for the network to be in Managed state, but may be required for other purposes.
5. The IPAM main page shows Yes as the value for the network under the Managed column. The network is now under management of IPAM and can participate in Infoblox services.

**Note:** Most conversion operations for networks and individual IP addresses are managed under IPAM and are described in the section Managing IPv4 and IPv6 Addresses of this Guide.

Converting Unmanaged IP Addresses to Managed Status

The principle for converting an IP address to managed status is the same for IP addresses as for interfaces. If an IP address is unmanaged but is present in IPAM, the IP can be converted to managed status.
1. From the **Data Management** tab, select the **Devices** tab.
2. Click the **Next Page** and **Last Page** icons to locate the device through which you want to locate the IP address to convert.
3. Click the Name of the device.
4. Click the **IP Addresses** tab for the chosen device. The IP address page lists all ports discovered on the selected device.
5. To **convert a single IP address**: Click the Action icon next to the IP address you want to convert (this automatically selects it), and then select **Convert**->**To Host**, **To A Record**, **To PTR Record**, or **To Fixed Address** from the menu.

**To convert multiple IP addresses (bulk conversion)**: Select the check boxes of the IP addresses you want to convert. From the Toolbar, select **Convert**->**To Host**, **To A & PTR Record**, or **To Fixed Address** from the menu.

6. **For a single IP address**: The respective object editor appears based on the conversion type you have selected. For example, if you select **To Host**, the Host editor appears. In the editor, define the required **General** settings for the new object. You can also define other settings you need from any of the tabs in the editor. For details about how to configure these settings, refer to the online Help in Grid Manager or see the appropriate chapters in this guide.

**For bulk conversion**: The respective bulk conversion wizard (such as the **Convert Unmanaged IP Addresses to Host Record** wizard) appears based on the conversion type you have selected.

**Note**: Network Insight creates the names of the new managed objects using the Discovered Name (FQDN) for the entities being converted. In the wizard, Grid Manager displays the IP addresses of the selected devices that are eligible for conversion in the **Selected IP Addresses** table. Entities that are not eligible for conversion will not be converted and will not appear in this table.

Based on the selected conversion type, complete the following to start a bulk conversion:

a. **To Host**: You can select **Enable in DNS** and/or **Enable in DHCP** so the appliance can serve DNS and/or DHCP for the selected IP addresses in the host record. When you enable DNS for the record, you must select a DNS zone for all entities that do not have an FQDN.

b. **To A&PTR Record**: Network Insight converts the selected entities to A & PTR records simultaneously. You must select a DNS zone for all entities that do not have an FQDN.

c. **To Fixed Address**: Network Insight automatically converts all selected IP addresses to fixed addresses in a bulk conversion. As with host record and A/PTR record conversions, entities without a Discovered Name FQDN are not eligible for conversions to fixed addresses.

In all bulk conversions, you can define extensible attributes for the selected IP addresses. After you have configured the necessary settings, you can convert the discovered entities immediately or schedule the conversion by selecting **Later** and entering the date and time. Click **Save & Close** to make the conversion. You can return to the managed object at any time to make further configuration changes.

7. In the **Managed** column for all converted entities, Grid Manager displays **Yes** to indicate the Managed status. The selected IP addresses are associated with the newly converted IPAM objects. You can now manage these IPAM objects through Grid Manager.

### Converting Unmanaged Assets to Managed Status

1. From the **Data Management** tab, select the **Devices** tab.
2. Click the **Next Page** and **Last Page** icons to locate the device through which you want to locate the assets to convert.
3. Click the Name of the device.
4. Click the **Assets** tab for the chosen device. The Assets page lists all network devices that have been detected through connections to the current device. If the device is a switch, you may see a list of end hosts and network servers in the list, along with any other network infrastructure devices that are neighboring the current device.
5. **To convert a single asset**: Click the Action icon next to the asset you want to convert (this automatically selects it), and then select **Convert --> To Host, To A Record, To PTR Record, or To Fixed Address** from the menu.

**To convert multiple assets (bulk conversion)**: Select the check boxes of the assets you want to convert. From the Toolbar, select **Convert --> To Host, To A & PTR Record, or To Fixed Address** from the menu.

6. **For a single asset** The respective object editor appears based on the conversion type you have selected. For example, if you select **To Host**, the Host editor appears. In the editor, define the required **General** settings for the new object. You can also define other settings you need from any of the tabs in the editor. For details about how to configure these settings, refer to the online Help in Grid Manager or see the appropriate chapters in this guide.

**For bulk conversion**: The respective bulk conversion wizard (such as the **Convert Unmanaged IP Addresses to Host Record wizard**) appears based on the conversion type you have selected.

**Note**: Network Insight creates the names of the new managed objects using the Discovered Name (FQDN) for the entities being converted. In the wizard, Grid Manager displays the IP addresses of the selected devices that are eligible for conversion in the **Selected I P Addresses** table. Entities that are not eligible for conversion will not be converted and will not appear in this table.

Based on the selected conversion type, complete the following to start a bulk conversion:

- **To Host**: You can select **Enable in DNS** and/or **Enable in DHCP** so the appliance can serve DNS and/or DHCP for the selected IP addresses in the host record. When you enable DNS for the record, you must select a DNS zone for all entities that do not have an FQDN.
- **To A & PTR Record**: Network Insight converts the selected entities to A & PTR records simultaneously. You must select a DNS zone for all entities that do not have an FQDN.
- **To Fixed Address**: Network Insight automatically converts all selected assets to fixed addresses in a bulk conversion. As with host record and A/PTR record conversions, entities without a Discovered Name FQDN are not eligible for conversions to fixed addresses.

In all bulk conversions, you can define extensible attributes for the selected assets. After you have configured the necessary settings, you can convert the discovered entities immediately or schedule the conversion for a later date by selecting **Later** and entering the date and time.

7. Click **Save & Close** to make the conversion. You can return to the managed object at any time to make further configuration changes. If you are in the **Managed** column for all converted entities, Grid Manager displays **Yes** to indicate the managed status. The selected assets are associated with the newly converted IPAM objects. You can now manage these IPAM objects through Grid Manager.

### About Automatic Conversion Rules

To automate the conversion of IP addresses of discovered entities from "unmanaged" to "managed" in a specific network view, you can configure conversion rules that Network Insight uses to automatically create new DNS records or update existing data for the discovered IP addresses. Network Insight automatically converts newly discovered IP addresses to host records, A and PTR records, or fixed addresses based on your configuration. You can define templates that Network Insight uses to create new records by using supported variables and functions. For information about supported variables, see **Supported Conversion Parameters**.

Note that corresponding DNS zones in a selected network view must already exist in order for Network Insight to add DNS records during the conversion. Otherwise, Network Insight does not add any DNS records and it logs a message to the syslog.

Network Insight automatically adds DNS records based on the following conditions:

- The corresponding DNS zones must already exist in the NIOS database. Network Insight does not automatically create DNS zones for the records.
- To create a PTR record, the corresponding reverse-mapping zone must exist.
- A DNS zone cannot be associated with more than one DNS view. Network Insight does not create DNS records for zones that are associated with multiple DNS views.
- NIOS adds new DNS records only if the discovered_name for the discovered IP address is available and there is no conflict with information about the associated network view.

On subsequent discovery jobs, if an IP for a VM is removed, the corresponding DNS records are removed accordingly. If the IP for a VM is changed, the IP address in the corresponding DNS record is changed accordingly. If the DNS record name template is changed, all the DNS records are replaced with the DNS records using the new template. All administrative actions for these changes are recorded in the audit log. Summary of the changes are logged in the syslog.

**Note**: Network Insight updates only records that are created by the Network Insight process. It does not create or update DNS records that are originally created by other admin users.

### Configuring Automatic Conversion Rules

To add automatic conversion rules:

1. From the **Grid** tab, select the **Grid Manager** tab, and click **Edit --> Grid Discovery Properties** from the Toolbar.
2. Click the **Conversion Policy** tab and complete the following:
   - **Enable the automatic conversion rules defined for newly discovered IP addresses**: Select this check box to enable the...
The automatic conversion of unmanaged IP addresses of newly discovered entities to managed objects in a specific network view is disabled by default.

- **Update discovered data for managed objects**: Select this check box if you want the appliance to update discovered data for all corresponding NIOS objects (if they exist in NIOS). If you do not select this check box, the appliance updates only the discovered data for unmanaged objects. None of the managed data will be updated. This check box is selected by default, but is disabled if you do not enable the automatic conversion feature.

Click the Add (+) icon and Grid Manager adds a row to the table (this table is enabled only when you enable the automatic conversion feature). Complete the following:

- **Network View**: From the drop-down list, select the network view in which your conversion rule will take effect. Note that this rule applies only to objects in the selected network view. If you have multiple network views, you must configure a separate policy for each network view.
- **Template**: Define a naming template that Network Insight uses to automatically create DNS records for the unmanaged IP addresses in the network view. You can use the following syntax: `${substitution}`, where substitution can be a supported variable or function. Note that each IPv6 address substitution is unwrapped into dotted presentation. For information about supported variables and functions, see Supported Conversion Parameters.

For example, when you enter `${discovered_name}.corpxyz.com` and the discovered_name for the asset is `XYZ`, the DNS name for this IP becomes `XYZ.corpxyz.com`. When you enter `$dev-{ip_address_octet3}.corpxyz.com` and the IP for the asset is `137.65.75.0/24`, the DNS name for this IP becomes `dev-3.corpxyz.com`. When you enter `${ip_address[7]}.corpxyz.com` for an IPv6 address and if the IP for the asset is `2001:db8:acad::1`, the DNS name becomes `b.corpxyz.com`. You can also use the following functions in the naming template: dashed, reversed, and underscored. For example, when you enter `@(dashed(${ip_address}))~corpxyz.com` and the IP is 1.2.3.4, the DNS name becomes `1-2-3-4~corpxyz.com`. When you enter `@(reversed(${ip_address}))~corpxyz.com` and the IP is 1.2.3.4, the DNS name becomes `4.3.2.1~corpxyz.com`.

- **Conditions**: Enter the matching conditions for the conversion rule. You can use magic variables, supported variables, operators, and functions in the condition. When Network Insight finds IP addresses that match this condition, it will convert the IP addresses into DNS records (Hosts, A/PTR records, or fixed addresses) based on your selected conversion type. For information about supported parameters, see Supported Conversion Parameters.

For example, if you want to match IP addresses that do not have an FQDN in the discovered_name, you can enter this condition: `${is_FQDN(${discovered_name})}==false AND ${discovered_name}=="unknown"`. If you want to match devices from the network `137.65.75.0/24` with the name starting with "Serial0"., you can enter this condition: `${ip_belongs_to("137.65.75.0/24")}==true AND ${discovered_name}like"Serial0"`.

**Conversion Type**: From the drop-down list, select the DNS record type that you want Network Insight to convert the unmanaged IP addresses into. You can convert an unmanaged IP into Host, A/PTR, or Fixed Address. When you select A/PTR, Network Insight converts each IP into A and PTR records simultaneously.

**Comment**: Enter description about this policy to distinguish it from others. For example, if the policy is used to identify and convert IP addresses with `discovered_name` that does not contain an FQDN, you can enter "No FQDN in discovered_name." as the comment to remind yourself about this conversion rule.

### Supported Conversion Parameters

The following tables list the supported magic variables, variables, operators, and functions that you can use to build the formula for the automatic conversion rules.

#### Table 15.1 Magic Variables for Conversion Rules

Some of the functions or predicates use the following magic variables to calculate the matching results.

<table>
<thead>
<tr>
<th>Name</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td><code>${ip_address}</code></td>
<td>The IP address. Used in is_ipv4, is_ipv6 predicates.</td>
</tr>
<tr>
<td>mgmt_ip_address</td>
<td><code>${mgmt_ip_address}</code></td>
<td>The management IP address. Used in is_interface predicate.</td>
</tr>
</tbody>
</table>

#### Table 15.2 Supported Variables for Conversion Rules

This tables lists all the variables you can use in the condition syntax.

<table>
<thead>
<tr>
<th>Name</th>
<th>Discovered by Network Insight</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>Y</td>
<td>Discovered IP address.</td>
</tr>
<tr>
<td>mac_address</td>
<td>Y</td>
<td>Discovered MAC address.</td>
</tr>
<tr>
<td>duid</td>
<td>Y</td>
<td>DUID associated with the IPv6 address.</td>
</tr>
<tr>
<td>netbios_name</td>
<td>Y</td>
<td>Discovered NetBIOS name.</td>
</tr>
<tr>
<td>os</td>
<td>Y</td>
<td>OS guessed by network discovery.</td>
</tr>
<tr>
<td>Field</td>
<td>Y/N</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>method</td>
<td>Y</td>
<td>The method being used for network discovery: FULL, ICMP, NETBIOS, TCP, or CSV.</td>
</tr>
<tr>
<td>network_component_type</td>
<td>Y</td>
<td>The type of network component, such as Switch, Router, and others.</td>
</tr>
<tr>
<td>network_component_name</td>
<td>Y</td>
<td>The name of the network component.</td>
</tr>
<tr>
<td>network_component_description</td>
<td>Y</td>
<td>A descriptive string for the network component.</td>
</tr>
<tr>
<td>network_component_ip</td>
<td>Y</td>
<td>IP Address of the network component.</td>
</tr>
<tr>
<td>network_component_port_number</td>
<td>Y</td>
<td>Port number on the network component on which the IP was discovered.</td>
</tr>
<tr>
<td>network_component_port_name</td>
<td>Y</td>
<td>Port name on the network component on which the IP was discovered.</td>
</tr>
<tr>
<td>network_component_vendor</td>
<td>Y</td>
<td>Vendor name of the network component to which the device is connected.</td>
</tr>
<tr>
<td>network_component_model</td>
<td>Y</td>
<td>Model name of the network component to which the device is connected in the vendor terminology.</td>
</tr>
<tr>
<td>network_component_port_id</td>
<td>Y</td>
<td>Interface ID of the connected switch/switch-router.</td>
</tr>
<tr>
<td>port_vlan_name</td>
<td>Y</td>
<td>Name of the VLAN on the port on the network component.</td>
</tr>
<tr>
<td>port_vlan_description</td>
<td>Y</td>
<td>Description of the VLAN on the port on the network component.</td>
</tr>
<tr>
<td>port_vlan_number</td>
<td>Y</td>
<td>Number of the VLAN on the port on the network component.</td>
</tr>
<tr>
<td>port_speed</td>
<td>Y</td>
<td>Speed settings on the port on the network component: 10M, 100M, 1G, 10G, 100G, or Unknown.</td>
</tr>
<tr>
<td>port_duplex</td>
<td>Y</td>
<td>Duplex settings on the port on the network component.</td>
</tr>
<tr>
<td>port_status</td>
<td>Y</td>
<td>Status of the port on the network component.</td>
</tr>
<tr>
<td>port_link_status</td>
<td>Y</td>
<td>Link Status of the port on the network component.</td>
</tr>
<tr>
<td>port_type</td>
<td>Y</td>
<td>Type of interface on the network component to which the device is connected.</td>
</tr>
<tr>
<td>open_ports</td>
<td>Y</td>
<td>List of opened ports on the IP address, represented as: &quot;TCP: 21,22,23 UDP: 137,139&quot;. Limited to max total of 1000 ports.</td>
</tr>
<tr>
<td>last_discovered_timestamp</td>
<td>Y</td>
<td>The timestamp when this data discovered.</td>
</tr>
<tr>
<td>first_discovered_timestamp</td>
<td>Y</td>
<td>The timestamp when this IP was first seen by the discovery station.</td>
</tr>
<tr>
<td>discovered_name</td>
<td>Y</td>
<td>Name of the IP as seen by the discovery station.</td>
</tr>
<tr>
<td>discoverer</td>
<td>Y</td>
<td>Name of the discoverer or Grid member.</td>
</tr>
<tr>
<td>device_vendor</td>
<td>Y</td>
<td>Vendor name of the device.</td>
</tr>
<tr>
<td>device_type</td>
<td>Y</td>
<td>Type of the device in the vendor terminology.</td>
</tr>
<tr>
<td>device_model</td>
<td>Y</td>
<td>Model name of the device in the vendor terminology.</td>
</tr>
<tr>
<td>mgmt_ip_address</td>
<td>Y</td>
<td>Management IP address of the device if the device has more than one IP.</td>
</tr>
<tr>
<td>device_port_name</td>
<td>Y</td>
<td>System name of the interface with which the IP associates.</td>
</tr>
<tr>
<td>device_port_type</td>
<td>Y</td>
<td>Hardware type of the interface with which the IP associates.</td>
</tr>
<tr>
<td>is_end_host</td>
<td>Y</td>
<td>Whether this object is an end host or an infrastructure device for the purpose of discovery.</td>
</tr>
<tr>
<td>iprg_id</td>
<td>Y</td>
<td>Port Redundant Group ID of this device interface.</td>
</tr>
<tr>
<td>iprg_no</td>
<td>Y</td>
<td>Port Redundant Group no of this device interface.</td>
</tr>
<tr>
<td>iprg_type</td>
<td>Y</td>
<td>Type of Port Redundant Group</td>
</tr>
<tr>
<td>iprg_state</td>
<td>Y</td>
<td>State of this IP address in the group.</td>
</tr>
<tr>
<td>vmi_name</td>
<td>N/A</td>
<td>Name of the virtual machine.</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>vmi_id</td>
<td>N/A</td>
<td>ID of the virtual machine.</td>
</tr>
<tr>
<td>vlan_port_group</td>
<td>N/A</td>
<td>Port group to which the virtual machine belongs.</td>
</tr>
<tr>
<td>vswitch_name</td>
<td>N/A</td>
<td>Name of the virtual switch.</td>
</tr>
<tr>
<td>vswitch_id</td>
<td>N/A</td>
<td>ID of the virtual switch.</td>
</tr>
<tr>
<td>vswitch_type</td>
<td>N/A</td>
<td>Type of the virtual switch: standard or distributed: Unknown, Standard, or Distributed</td>
</tr>
<tr>
<td>vswitch_ipv6_enabled</td>
<td>N/A</td>
<td>Indicates whether the virtual switch has IPV6 enabled: true or false</td>
</tr>
<tr>
<td>vport_name</td>
<td>N/A</td>
<td>Name of the network adapter on the virtual switch connected with the virtual machine.</td>
</tr>
<tr>
<td>vport_mac_address</td>
<td>N/A</td>
<td>MAC address of the network adapter on the virtual switch to which the virtual machine is connected.</td>
</tr>
<tr>
<td>vport_link_status</td>
<td>N/A</td>
<td>Link status of the network adapter on the virtual switch to which the virtual machine is connected.</td>
</tr>
<tr>
<td>vport_conf_speed</td>
<td>N/A</td>
<td>Configured speed of the network adapter on the virtual switch to which the virtual machine is connected. Unit is Kib.</td>
</tr>
<tr>
<td>vport_conf_mode</td>
<td>N/A</td>
<td>Configured mode of the network adapter on the virtual switch to which the virtual machine is connected: Unknown, Full-duplex, or Half-duplex</td>
</tr>
<tr>
<td>vport_speed</td>
<td>N/A</td>
<td>Actual speed of the network adapter on the virtual switch to which the virtual machine is connected. Unit is Kib.</td>
</tr>
<tr>
<td>vswitch_segment_type</td>
<td>N/A</td>
<td>Type of network segment on which the current virtual machine/vport is connected.</td>
</tr>
<tr>
<td>vswitch_tep_ip</td>
<td>N/A</td>
<td>IP address of the virtual tunnel endpoint (VTEP) in the virtual switch.</td>
</tr>
<tr>
<td>vswitch_tep_port_group</td>
<td>N/A</td>
<td>Port group of the virtual tunnel endpoint (VTEP) in the virtual switch.</td>
</tr>
<tr>
<td>vswitch_tep_vlan</td>
<td>N/A</td>
<td>VLAN of the virtual tunnel endpoint (VTEP) in the virtual switch.</td>
</tr>
<tr>
<td>vswitch_tep_dhcp_server</td>
<td>N/A</td>
<td>DHCP server of the virtual tunnel endpoint (VTEP) in the virtual switch.</td>
</tr>
<tr>
<td>vswitch_tep_multicast</td>
<td>N/A</td>
<td>Multicast address of the virtual tunnel endpoint (VTEP) in the virtual switch.</td>
</tr>
<tr>
<td>vmhost_ip_address</td>
<td>N/A</td>
<td>IP address of the physical node on which the virtual machine is hosted.</td>
</tr>
<tr>
<td>vmhost_name</td>
<td>N/A</td>
<td>Name of the physical node on which the virtual machine is hosted.</td>
</tr>
<tr>
<td>vmhost_mac_address</td>
<td>N/A</td>
<td>MAC address of the physical node on which the virtual machine is hosted.</td>
</tr>
<tr>
<td>vmhost_subnet_cidr</td>
<td>N/A</td>
<td>CIDR subnet of the physical node on which the virtual machine is hosted.</td>
</tr>
<tr>
<td>vmhost_nic_names</td>
<td>N/A</td>
<td>List of all physical port names used by the virtual switch on the physical node on which the virtual machine is hosted. Represented as: eth1,eth2,eth3.</td>
</tr>
<tr>
<td>vmi_tenant_id</td>
<td>N/A</td>
<td>ID of the tenant to which the virtual machine belongs.</td>
</tr>
<tr>
<td>cmp_type</td>
<td>N/A</td>
<td>If the IP is coming from a Cloud environment, the Cloud Management Platform type.</td>
</tr>
<tr>
<td>vmi_ip_type</td>
<td>N/A</td>
<td>Discovered IP address type.</td>
</tr>
<tr>
<td>vmi_private_address</td>
<td>N/A</td>
<td>Private IP address of the virtual machine.</td>
</tr>
<tr>
<td>vmi_is_public_address</td>
<td>N/A</td>
<td>Indicates whether the IP address is a public address.</td>
</tr>
<tr>
<td>cisco_ise_ssid</td>
<td>N/A</td>
<td>Service Set Identifier.</td>
</tr>
<tr>
<td>cisco_ise_security_group</td>
<td>N/A</td>
<td>Name of the security group created in Cisco ISE.</td>
</tr>
<tr>
<td>cisco_ise_quarantine_status</td>
<td>N/A</td>
<td>Quarantine status for the IPAddress as coming from Cisco ISE: NONE or QUARANTINE</td>
</tr>
<tr>
<td>cisco_ise_endpoint_profile</td>
<td>N/A</td>
<td>Endpoint profile in Cisco ISE.</td>
</tr>
</tbody>
</table>
Table 15.3 Supported Operators for Conversion Rules

Operators always result in boolean value: true or false. Therefore, you can use them only in logical expressions.

<table>
<thead>
<tr>
<th>Name</th>
<th>Left Value (lvalue)</th>
<th>Right Value (rvalue)</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIKE</td>
<td>variable</td>
<td>string (regular expression in extended format)</td>
<td><code>${discovered_name} like &quot;[vV]m-[0-9]+.devnet.org&quot;</code></td>
<td>Evaluates as true if the lvalue variable matches the given regular expression rvalue; otherwise false</td>
</tr>
<tr>
<td>==</td>
<td>variable</td>
<td>string</td>
<td><code>${ip_address} == &quot;167.45.13.29&quot;</code></td>
<td>Evaluates to true if the lvalue variable equals to rvalue string literal, false otherwise</td>
</tr>
<tr>
<td>!=</td>
<td>variable</td>
<td>string</td>
<td><code>${mac_address} != &quot;00:50:56:00:00:01&quot;</code></td>
<td>Evaluates to true if the lvalue variable is not equal to rvalue string literal, false otherwise</td>
</tr>
</tbody>
</table>

Table 15.4 Supported Functions or Predicates for Conversion Rules

Predicates accept either none or one argument. Depending on the predicate, it could accept both variables and strings or only one of them. The predicate can be compared only to boolean value: true or false.

<table>
<thead>
<tr>
<th>Name</th>
<th>Argument Type</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>is_interface</td>
<td>N/A</td>
<td>${is_interface} == true</td>
<td>Check discovered data in an interface. It validates the mgmt_ip_address variable.</td>
</tr>
<tr>
<td>is_ipv4</td>
<td>N/A</td>
<td>${is_ipv4} == true</td>
<td>Check to see if the variable ip_address is an IPv4 address.</td>
</tr>
<tr>
<td>is_ipv6</td>
<td>N/A</td>
<td>${is_ipv6} == false</td>
<td>Check to see if the variable ip_address is an IPv6 address.</td>
</tr>
<tr>
<td>is_belongs_to</td>
<td>string</td>
<td>${ip_belongs_to(&quot;10.0.0.0/8&quot;)} == false</td>
<td>Check to see if the ip_address variable belongs to the given IPv4 or IPv6 network range.</td>
</tr>
<tr>
<td>is_fqdn</td>
<td>variable</td>
<td>${is_fqdn(${discovered_name})} == true</td>
<td>Check to see if the given variable is an FQDN.</td>
</tr>
</tbody>
</table>

Viewing Discovered Devices and their Properties

Note: For information about unmanaged devices and managed devices and what their respective status means, see Converting Unmanaged Devices to Managed Devices. You can also use the "Unmanaged devices and networks" filter in global search to locate all the unmanaged devices and networks discovered through discovery. For more information, see Using Global Search.

After discovery begins executing on the network, Grid Manager provides a Devices page under Data Management for a complete list of every device that discovery finds, and lists all unmanaged and managed devices. Starting here, you can explore a substantial body of information about the complete list of discovered and managed devices, and drill down to specific information about every discovered and managed device. Listed devices inhabit one of three states in the Devices page:

- Devices that appear with an empty value in the Managed column are devices that are discovered, but are not recognized by IPAM, are not part of an IPAM network, and hence cannot be changed to managed status in Grid Manager. These discovered devices cannot be changed to managed status, but you can perform actions such as activating and deactivating ports, executing Discover Now on the device, view their list of connected networks, and other actions. Avoid changing the state of ports or taking other actions on a discovered device, unless the action is verified by an administrator.
- Device shown in yellow table rows are unmanaged devices, but are recognized by IPAM and can be converted to managed status. Yellow rows appear with a value of No in the Managed column. You can convert devices in table rows to managed objects under IPAM (host, fixed address. A record or PTR record);
- Devices shown in light grey table rows are managed devices, with a value of Yes in the Managed column.

Viewing the Complete List of Discovered Devices

The Data Management tab → Devices tab provides a complete view of all discovered devices discovered by Network Insight. The list includes routers, switches, firewalls and other security devices, wireless APs, end hosts and servers in end-host networks. Use NIOS standard filtering to narrow down the status table to the devices or values you want to examine.

In the viewer, click the Action icon 🌎 for any table row to view the following:

- Click Show IPAM Address to open the IPAM status page to view records information for the Router IP address, and information such as any IPAM/DHCP objects associated with the IP address (RelatedObjects) and its recent history in Grid Manager (AuditHistory).
• Click Interfaces to display the complete table of interfaces associated with the network device.
• Click IPAM Networks and choose any network prefix in the list. The IP Map page appears for the chosen network for which the device is a part.
• Click Edit to open the device editor, to change settings for interfaces on the selected device; apply extensible attributes, or apply administrative permissions for Grid Manager admin access to a device.
• Choose DiscoverNow to apply discovery to a listed device to detect configuration changes, status changes and other device information.
• Where applicable, choose Convert to change the status of an unmanaged device to managed status under Grid Manager. (For more information, see Converting Unmanaged Networks under IPAM to Managed Status.)
• Click Device Details to view a short list of key information about the selected device.
• Click Device Support to verify data collection activities in the following tabs:
  • Data Collection: You can view the timestamp at which the most recent collection from various data sources was completed. The sources from which device support information is collected are listed under the Data Source column, and it includes the device’s routing table (ipRouteTable), environment monitoring (DeviceEnvMon), and numerous other data sources as applicable to the specific device type. It displays the following information for each discovered device:
    ▪ Data Source: The sources from which the device support information was collected.
    ▪ End Time: The most recent timestamp of the data collected by the discovery member.
• Device Support tab: Lists various types of information supported for collection on the current device. You can view the following details for each discovered device:
  • Function: Data function that can be collected by Network Insight. The value can be Device Vendor, Device Model, Device Version, VLANs, Forwarding, VRFs, Inventory, and Security Control.
  • Supported: Indicates whether this data function is supported for the selected device. The value can be Yes or No. If it is No, Network Insight will not attempt to gather the data. For instance, for a Cisco router, Network Insight does not attempt to gather VLAN information, so a No value will be displayed in the Supported column.
  • Available: Reflects whether the data has actually been collected. The value can be Yes or No. A value of Yes for Supported and No for Available indicates a discovery misconfiguration or could possibly require an adjustment to the Device Support Bundle (DSB) for that particular device model.
  • Value: Displays the value collected for the Device Vendor, Device Model, and Device Version data functions. Displays Last Collected time for the VLANs, Forwarding, VRFs, Inventory, and Security Control data functions.
• Click ShowActiveUsers to view all the active users on the Active Directory domain for the selected device. For information, see Viewing Active Network Users.

Values listed in the Discovered Devices table include the following:

• IP Address: Detected the IP address (IPv4 or IPv6).
• Name: Detected name of the device. Each device name provides a link to the complete body of information associated with the device, arranged in five tabs: Interfaces, Networks, IP Addresses, Assets and Components. For more information, see the sections under Accessing Detailed Device Information.
• Device Type: The network device type: Router, Switch-Router, Firewall, NIOS (Infoblox appliance), vNIOS, SDN Controller, SDN Element, and others.
• Model: The model name as detected by the device during discovery.
• Serial Number: The serial number of the discovered device.
• Vendor: The equipment manufacturer (Cisco, Juniper, Fortinet, F5, and others);
• Device Version: The Operating System version for the network device.
• Chassis S/N: The chassis serial number of the discovered device.
• Location: The physical location of the network device as detected by the device during discovery.
• Description: Verbose description of the network device as collected from the device by discovery.
• Discover Now: Indicates when the device is undergoing a current discovery process. A “Pending” icon appears in this column to indicate the status.
• Managed: Indicates the status of the device in Grid Manager. A blank value in this field indicates the device has been discovered but is not recognized in IPAM; a No value indicates the device is recognized by IPAM but is not managed under Grid Manager; and a Yes value indicates that the device is fully managed by Grid Manager from use of the Convert command and can support related features such as port reservations and IPAM/DHCP object assignments. (For more information, see Converting Unmanaged Networks under IPAM to Managed Status.)
• Active Users: The number of active users on the Active Directory domain for the selected IP address.

Click Discovery Status in the Toolbar to view the same list of network devices showing the discovery data set. You can sort the table by Name or IP address. Use Grid Manager-standard filtering to isolate device names, IP addresses or other values in which you are interested.

For each listed device, the Action icon

 PROVIDES THE FOLLOWING OPTIONS DEPENDING ON THE DEVICE TYPE AND ITS STATUS:
• Interfaces: Displays the Interfaces page for the chosen device. (For more information, see Viewing Networks Associated with Discovered Devices.)
• Show IPAM IP Address: Shows the Management IP address for the device that has a network in IPAM—the main IPAM tab appears, showing details for the IP address. This option is greyed out for devices that have a management IP that is not part of an IPAM network;
• Edit: Displays the Device Editor window:
  • Interfaces: A direct link to the Interfaces page for the chosen device. Unmanaged devices may have managed interfaces that appear in this page, and managed devices may have unmanaged interfaces that appear here;
• Discover Now: Directs Network Insight to immediately perform discovery on the selected device;
• Convert: For devices in unmanaged status (shown in yellow), allows conversion of the device to a managed object in Grid Manager: a host, fixed address, A record or PTR record. (For more information, see Converting Unmanaged Devices to Managed Devices.)
**Networks**: A drop-down list of all IPv4/IPv6 IPAM networks currently provisioned on the device. Each network provides a link to the IP Map page for the selected network.

**Device Details**: A basic list of information about the chosen device, including the IP address by which the device is discovered, operational status, IPAM Type (whether the device is managed or unmanaged), the Device Type and the number of Interfaces.

**Show Active Users**: Displays the Active Users dialog box. You can view all the active users on the Active Directory domain for the selected device. For more information, see Viewing Active Network Users.

**Viewing Discovered VRFs and Mapping Network Views**

To view VRF instances (or VRFs) and map corresponding network views, do the following:

1. From the Data Management tab, select the Devices tab, and then click VRF Mapping from the Toolbar.
2. The VRF Mapping dialog appears and displays the following:
   - **VRF Name**: The name of the VRF on the hosting device, which typically contains the interface name and its VRF route distinguisher.
   - **Device Name**: The discovered name of the device that is hosting the VRF.
   - **Device IP Address**: The IP address of the managed VRF hosting device.
   - **Network View**: The network view that is associated with the VRF. You can click this field and select a different network view from the drop-down list.

You can do the following in this tab:

- To assign the same network view to multiple VRFs, select the check boxes of the VRFs, and then click the Edit icon. The VRF Mapping dialog displays the Edit VRF Network View panel. From the Network View drop-down list, select the network view you want to assign to all the selected VRFs, and then click Save. If there is only one network view in the Grid, which is the default view, the Network View column is hidden by default.
- You can use filters to narrow down the list. You can filter the list based on the VRF name, Device name, Device IP address, and network view. For more information, see Using Filters.
- You can sort the data in ascending or descending order by column.

**Note**: The appliance displays a warning message when there are discovered VRFs that are not mapped to network views. To ensure that discovered VRFs are mapped to network views, you can configure automatic VRF mapping, as described in Configuring Automatic VRF Mapping.

**Accessing Detailed Device Information**

Clicking on any device’s name in the Name column, you open a set of five tabs revealing information about the selected device (see the following sections for details on discovered and managed devices):

- The Interfaces tab (see Viewing Interface Information for Discovered Devices below);
- The Networks tab (see Viewing Networks Associated with Discovered Devices);
- The IP Addresses tab (see Viewing IP Addresses Associated with Discovered Devices);
- The Assets tab (see Viewing Assets Associated with Discovered Devices);
- The Components tab (see Viewing Components of Discovered and Managed Devices).

**Viewing Interface Information for Discovered Devices**

This panel lists all discovered interfaces associated with the selected device. Interfaces are detected whether they are loopbacks, unnumbered, or numbered with one or more IP addresses. Interfaces may be listed for either managed or unmanaged devices.

1. From the Data Management tab, select the Devices tab. The Devices Home page displays a list of all devices currently found and catalogued by discovery.
2. Click the Action icon 💡 for a chosen device and choose Interfaces from the drop-down menu, or simply click the device name to display the Interfaces list. Click Devices Home to return to the main Devices page.

This panel displays the following information for each interface. Note that some data may appear for some device types and not for others.

- **Name**: The name of the interface (usually a switched interface) associated with the discovered device.
- **Reservation**: Indicates whether the port has been reserved by NIOS as part of a Port Control operation.
- **IP Address**: Detected IPv4 or IPv6 address of the interface.
- **VRF Name**: The name of the VRF associated with the interface, if applicable.
- **Network View**: The name of the network view to which the VRF instance belongs, if applicable. If there is only one network view in the Grid, which is the default view, the Network View column is hidden by default.
- **VRF Description**: The description about the VRF instance, if applicable.
- **VRF RD**: The route distinguisher associated with the VRF instance, if applicable.
- **MAC Address**: The hardware address associated with the interface.
• **Description:** Port description associated with the interface, such as `ge-0/0/5` or `FastEthernet0/13`.
• **VLAN ID/VLAN Name:** The data VLAN identifier and VLAN name that is bound to the interface, if applicable.
• **Port Speed:** Interface speed, in Mbps.
• **Port Type:** Type of interface as detected by NIOS Discovery. Examples include `ethernet-csmacd`, `propPointToPoint Serial`, `I2 vlan`, and others.
• **Admin Status:** Shows whether the interface is administratively Up or administratively Down.
• **Operating Status:** Shows whether the interface is operationally Up or operationally Down.
• **Trunk Status:** Where applicable, shows the trunking status of the interface.
• **Link Aggregation:** Shows the state of the interface if it is part of a LAG (Link Aggregation Group).
• **Status:** Shows whether the interface is Used or Unused.
• **IPAM Type:** The object type that is associated with the IP address for the interface. Possible values can be Lease, IPv4 DHCP Range or Fixed Address.
• **Usage:** Indicates whether NIOS has configured the IP address for DNS or DHCP.
• **Managed:** Shows whether the interface is managed under IPAM, by being associated with a managed IPAM object such as a Fixed Address. Check the IPAM Type field for related information.
• **Reservation:** Indicates whether the interface has a port reservation bound to it. For information, see Creating Port Reservations for IPAM Objects.
• **Capabilities:** Describes the capabilities of each interface in the selected device. Hover the mouse over each entry to view the complete listing. For information, see Determining Interface Capabilities.
• **Site:** This is a predefined extensible attribute.

You can also click the Action icon next to an interface name and select one of the following to perform the specified task:

- **Edit:** This option is enabled if the network is in managed state. This opens the network editor.
- **Show Assets:** This option is only available for switched Ethernet interfaces with no IP Address. This opens the Assets page for the selected device, and shows a list of end host devices or neighboring linked to the interface. Network Insight filters the asset list for the device by the interface name.
- **Show Multiple IP Addresses:** Opens the IP Addresses page specifically for the interface, listing all IPv4 and IPv6 addresses associated with the interface. This option appears only if the interface has IP addresses.
- **Convert:** Convert a network in the unmanaged state to be managed under IPAM and (optionally) DHCP. Unlike devices and interfaces, you do not assign objects such as fixed addresses or PTR records to a managed network. Conversion enables a network to be fully manageable under IPAM and DHCP. For more information, see Converting Unmanaged Networks to Managed Status.
- **IPAM Networks:** Choosing this option lists all IPAM networks associated with the current interface.
- **Device Details:** A basic list of information about the chosen device, including the IP address by which the device is discovered, operational status, IPAM Type (whether the device is Managed or Unmanaged), the Device Type and the number of Interfaces.

You can also do the following:

- Modify some of the data in the table. Double click a row, and either modify the data in the field or select an item from a drop-down list. Click **Save** to save the changes or click **Cancel** to exit. Note that some fields are read only. You can modify the following fields in this table: **VLAN ID/VLAN Name**, **Admin Status** and **Description**.
- Sort the data in ascending or descending order by column.
- Select an interface check box and click the Edit icon to manage device properties.
- Click the Export icon to export the list of discovered devices to a `.csv` file.
- Click the Print icon to print the list of discovered devices.
- Use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of a device name in the **Go to** field and select the device from the possible matches.
- Create a quick filter to save frequently used filter criteria.

### Determining Interface Capabilities

One key piece of information that Network Insight compiles from discovery involves an assessment of interface capabilities. The Interfaces table provides a hidden column titled **Capabilities** with a description of the relevant capabilities of each interface in the discovered device.

1. From the **Data Management** tab, select the **Devices** tab. The Devices Home page displays a list of all devices currently found and catalogued by discovery.
2. Click the Action icon

   ![Action Icon](image)

   for a chosen device and choose **Interfaces** from the popup menu.
3. Click the right end of a column header and choose **Columns** → **Edit Columns** from the drop-down menu.
4. Select the **Capabilities** check box and click **Apply**.

The text listing for the Capabilities field may be too long to display in the Interfaces table. Hover the mouse over any table row to display the complete entry for the **Capabilities** field:

Figure 15.7 Capabilities information for the selected interface
Critical values in the Capabilities field include the following:

- Provision IPv4 Network – Yes or No
- Provision IPv6 Network – Yes or No
- De-Provision IPv4 Network – Yes or No
- De-Provision IPv6 Network – Yes or No
- Interface has no IP Address – Appears only if no IP address is defined for the interface
- Edit Data VLAN – Yes or No
- Edit Voice VLAN – Yes or No
- Edit Admin Status – Yes or No
- Edit Description – Yes or No

The values you see in this field provide notification when you are unable to set certain values for any interface. When discovery queries devices for their device type, OS version support and other factors, Network Insight compiles the information into table formats that help you to determine issues or exceptions in the network.

For example, loopback interfaces are "always up" and hence do not support an Admin Status configuration and show Edit Admin Status = No. If an interface does not have an IP address, it cannot be de-provisioned and hence shows a De-provision Network = No. That same device may not support IP addresses or VLANs because it is only a L2 Ethernet switch, and shows Edit VLAN = No and Provision IPv4 Network = No, among others.

If a device shows a Provision IPv4 Network = Yes and Provision IPv6 Network = No, it indicates that the device supports only IPv4, perhaps due to OS software version.

Other cases may involve the following reasons:

- **Edit Admin Status = No:**
  - Device not supported
  - Vendor not supported
  - Model not supported
  - Port does not support Admin settings (Loopback, Virtual)

- **Edit VLAN = No:**
  - Device not supported
  - Device type not supported for VLAN assignment (Router, L2 switch)
  - Vendor not supported
  - Model not supported

- **Edit Voice VLAN = No:**
  - Device not supported
  - Vendor not supported (Cisco is the only supported device type)
  - Device not licensed
  - Model not supported

- **Provision IPv4 Network=No/Provision IPv6 Network=No:**
  - Device not supported
  - Vendor not supported for network provisioning

- **De-Provision IPv4 Network=No/De-Provision IPv6 Network=No:**
  - Device not supported
  - Vendor not supported for network provisioning
  - Device type not supported for network provisioning (Router)

- **Edit Description=No**
  - Device not supported
  - Vendor not supported
  - Model not supported

**Viewing Networks Associated with Discovered Devices**

To view all discovered networks associated with the selected device, complete the following:

1. From the Data Management tab, select the Devices tab. The Devices Home page displays a list of all devices currently found and catalogued by discovery.
2. Click the Action icon
   - for a chosen device and choose Interfaces from the drop-down menu, or simply click the device name to display the Interfaces list. Click Devices Home to return to the main Devices page.
3. Click the Network tab. Grid Manager displays all networks to which the chosen device connects. The Networks page uses the same conventions as the main IPAM page for network listings.

You see three types of networks in this page:

- Networks shown in grey table rows are discovered networks that cannot be added to IPAM because they do not fit within the list of currently configured or discovered networks. (These networks are also called Non-NIOS networks.) Grey rows appear with an empty value in the Managed column. When a network is in this state you are limited to de-provisioning discovered networks of this type from their host device, and viewing device details.
- Networks shown in yellow table rows are unmanaged networks, but are recognized by IPAM and can be converted to managed status. Yellow rows appear with a value of No in the Managed column. You can provision these networks onto devices;
- Networks shown in white table rows are managed networks, appearing with a value of Yes in the Managed column. You can provision and de-provision managed networks.

Grid Manager displays the following applicable information for each network found on the selected device. A field is left blank if the information is not applicable to the network.

- **Network**: The network IPv4 or IPv6 address.
- **VRF Name**: The name of the VRF associated with the interface, if applicable.
- **Network View**: The name of the network view to which the VRF instance belongs, if applicable. If there is only one network view in the Grid, which is the default view, the Network View column is hidden by default.
- **VRF Description**: The description about the VRF instance, if applicable.
- **VRF RD**: The route distinguisher associated with the VRF instance, if applicable.
- **Comment**: Any information entered by admins about the network.
- **Managed**: Shows values of Yes or No for managed status.

Using the Action icon 

, you can perform the following tasks in the Networks page:

- **Show IPAM Network**: Opens the IPAM IP MAP that illustrates the IP states for all IPs in the network.
- **De-provision Network**: Available for managed networks that are provisioned and active on a device. Allows you to de-provision (delete) the selected IPAM network from all devices connected to the selected network. See Provisioning and De-Provisioning Networks.
- **Edit**: Opens the network editor for the selected network. This option is enabled if the network is in managed status.
- **Delete**: Select Delete to delete the network now or select Schedule Deletion to schedule the deletion at a later time. Note that the deletion function allows you to de-provision the actual network from the device. By default, when you choose Delete or Scheduled Delet e, the network is de-provisioned from all interfaces listed in the panel. Exercise caution when using this feature!
- **Extensible Attributes**: Provides access to the extensible attribute settings for the selected network.
- **Permissions**: Provides access to admin permissions settings for the selected network. This option is enabled if the network is in managed status.
- **Convert**: Converts unmanaged network to a managed network in NIOS. All discovered networks on each device are automatically listed as Unmanaged after a discovery. This means that the discovered network, though visible, does not have its identities resolved by NIOS, nor are its IP address managed through IPAM or leased through DHCP. After converting the unmanaged network to managed status, Grid Manager uses the discovered router IP address to populate the same value under subsequent DHCP configurations for the network. You can also select an unmanaged network and convert it to managed status by clicking Convert from the Toolbar.
- **Device Details**: Provides information about the device to which the selected network belongs. The list includes information such as the IP Address and Device Type for the device, and in the IPAM Type field whether the device itself is a managed or unmanaged object in NIOS. It also provides the following status counters for the device:
  - **Administrative Up - Operational Up**: The number of ports that are fully up and passing traffic
  - **Administrative Up - Operations Down**: The number of ports that are administratively up, but have some kind of connectivity issues.
  - **Administrative Down - Operational Down**: The number of ports that are administratively taken down.

The horizontal navigation bar and the Toolbar also provide the following functions:

- **Provision Network**
  : Available for managed networks and for unmanaged networks that are recognized by IPAM. For information, see Provisioning and De-Provisioning Networks. Clicking this icon opens the Provision Network feature, allowing you to provision the network onto the actual device by selecting a device interface, and enabling DHCP Forwarding and/or assigning a VLAN. Grid Manager creates a new port control task under Task Manager, and you can choose the interface on which the network is provisioned, along with VLAN configuration and other settings.
- **De-Provision Network**
  : Available for discovered networks that are not visible under IPAM. A dialog box appears summarizing the task.
- **Show Active Users**: For Microsoft Management only. Displays the Active Users dialog box. You can view all the active users on the Active Directory domain for the selected device. For more information, see Viewing Active Network Users.

Modifying Networks

Grid Manager enables the user to edit select DHCP configurations, including the following:
1. IPv4 DHCP Options/IPv6 DHCP Options: DHCP options provide specific configuration and service information to DHCP clients. For more information, see About IPv4 DHCP Options.

2. DHCP Forwarding: Enables routers connecting multiple networks to act as a silent DHCP relay and forward DHCP packets between them. The DHCP Forwarding page lists the interfaces on the currently selected network on which DHCP Forwarding is enabled. If more than one device on the selected network also enables DHCP Forwarding, they also appear here. DHCP Forwarding configuration involves simply enabling or disabling the service for a network endpoint on the device. In order for DHCP forwarding to work, you must restart the DHCP service on the Grid member that is serving the network. If you run DHCP service on both LAN1 and LAN2 of the Grid member, then both addresses are written to the device.

3. From the Data Management tab, select the Devices tab.
4. Click the Name link for the device you want to inspect.
5. Click the Networks tab.
6. Click the Action icon

   for a network in the table, and choose Edit. This feature is enabled only for networks that are managed under IPAM.

7. Click the DHCP Forwarding tab.
8. Select the check box for any listed instance and do the following if necessary:
   - Click Configure. Grid Manager queries you to confirm that DHCP Forwarding are configured on the selected network (A task will be created to configure DHCP forwarding for this network on these devices: <device_name>. You can view the execution log for the task in the Task Manager to see the results).
   - Click Delete to remove the selected DHCP Forwarding instance from the network.

Figure 15.8 DHCP Forwarding confirmations

1. Click Yes to confirm the activating or deletion of DHCP forwarding on the selection, or No to reject the change.
2. Click Save & Close.

Viewing IP Addresses Associated with Discovered Devices

You can view the complete list of discovered IP addresses bound to all interfaces for any device, discovered and managed devices alike.

Note: One useful trick for interfaces is to pick out an interface from the Interfaces page that has multiple IPs and open the IP Addresses tab; or sort the IP addresses table by its IP Address column, and locate the interface name that bears multiple IPs. Frequently, an interface with multiple addresses can have IPv4 and IPv6 addresses bound to it. Loopbacks are another example.

1. From the Data Management tab, select the Devices tab. The Devices Home page displays a list of all devices currently found and cataloged by discovery.
2. Click the Action icon

   for a chosen device and choose Interfaces from the drop-down menu, or simply click the device name to display the Interfaces list. Click Devices Home to return to the main Devices page.
3. Click the IP Addresses tab. Grid Manager displays all IP addresses associated with the chosen device. Grid Manager displays the following information for each IP address:
   - **IP Address**: The IP address for each discovered interface as managed by NIOS and IPAM. The table supports IPv4 and IPv6 values. Each IP address is a link to the home IPAM page for the interface. If an IP address does appear but is not a link, this indicates the discovered IP is not recognized under IPAM.
   - **VRF Name**: The name of the VRF associated with the interface, if applicable.
   - **Network View**: The name of the network view to which the VRF instance belongs, if applicable. If there is only one network view in the Grid, which is the default view, the Network View column is hidden by default.
   - **VRF RD**: The route distinguisher associated with the VRF instance, if applicable.
   - **Interface Name**: The name of the interface (usually a switched interface) associated with the discovered device.
   - **MAC Address**: The hardware MAC address associated with the interface.
   - **VLAN Name/VLAN ID**: The data VLAN name and VLAN identifier to which the interface is bound, if applicable. In most cases, you see both the VLAN name and the VLAN ID as two values in the same field. Multiple VLAN entries may be present for an interface or IP Address. Some interfaces may have a large
number of associated VLANs. By default, Network Insight does not automatically show all of them, instead providing a Show all... link for reference within the table cell. All VLAN ID/VLAN name values appear within the table cell, with a Hide... link provided to shorten the list back to original length.

- **AdminStatus**: Lists whether the interface is administratively Up or administratively Down.
- **OperationStatus**: The operational status of the interface (operationally Up or operationally Down).
- **Managed**: Indicates whether or not the IP Address is managed by Grid Manager. If the IP address is unmanaged, you will be able to Convert the IP address to an Object that is managed by Grid Manager.
- **Site**: This is a predefined extensible attribute. Extensible attributes may also appear in this table.

4. Click the IP Address link for any interface to open the Related Objects page for the chosen port.

Click the Action icon

next to an IP address and select one of the following to perform the specified task. Note that some of these actions are not applicable to the IP address.

- **Edit Interface**: Opens the interface general settings page. You can view and modify basic interface settings such as **Admin Status** (on the General page), **Data VLAN** and **Voice VLAN** (on the VLAN page), and add or modify extensible attributes.
- **Convert**: Depending on the address type and its IPAM status, you may be able to convert the selected IP to a Host Record, A Record, PTR Record or a Fixed Address. Otherwise, Grid Manager shows This object cannot be converted. You can also perform the same action by selecting an IP address check box and clicking Convert from the Toolbar.
- **Device Details**: Provides information about the device to which the selected IP address belongs. The list includes information such as the **IP Address** and **Device Type** for the device, and in the **IPAM Type** field whether the device itself is a managed or unmanaged object in NIOS. It also provides the following status counters for the device:
  - **Total Available Interfaces**: The total number of interfaces associated with the device.
  - **Administrative Up - Operational Up**: The number of ports that are fully up and passing traffic
  - **Administrative Up - Operational Down**: The number of ports that are administratively up, but have some kind of connectivity issues.
  - **Administrative Down - Operational Down**: The number of ports that are administratively taken down.

### Viewing Router Redundancy Information

Some discovered devices may support router redundancy. After discovery, some IP addresses are indicated as a VIP (virtual IP) in the device's IP Addresses page with router redundancy. In the IP List page, **Router Redundancy** in the Action icon menu lists the IP addresses associated with the VIP. For each IP, there are various menu items as shown in **Figure 15.9**.

*Figure 15.9 Virtual IPs and discovered redundancy information*

- **Active**: lists the active interface in the redundancy pair;
- **VIP**: The Virtual IP for the router redundancy pair;
- **Standby**: The standby IP interface for the router redundancy.

Discovery of all three IP components of the Router Redundancy instance also provides related information for all three IP entities:

- **Show IPAM Address**: opens the IPAM page to the listed IP address;
- **VIP**: Opens the virtual interface in the host device's Interfaces page;
- **Device name**: The third item lists the device name of the router for each of the three IP address entities comprising the redundancy instance. The currently active router is identified with the **Active** and VIP objects; the second **Standby** router is identified with the **Standby** IP address.

### Viewing Assets Associated with Discovered Devices

During discovery, Network Insight classifies end hosts and any other devices connected to switchport interfaces as "Assets" directly associated with each discovered interface. On the device level, the Assets page shows all network devices reachable by the selected network device, including switchports supporting end hosts. In practice, most Asset tables show end hosts and devices that populate Ethernet network segments. The Assets table lists all managed end hosts and application servers detected through discovery and identity resolution by Grid Manager, that are connected to each network infrastructure device. The records listed in this table date from the Last Seen discovery time stamp of each end host or other device. In many cases, you see neighbor devices to the current device appearing on this page.

To view assets associated with discovered devices:

1. From the **Data Management** tab, select the **Devices** tab. The Devices Home page displays a list of all devices currently found and catalogued by discovery.
2. Click the Action icon

for a chosen device and choose **Interfaces** from the drop-down menu, or simply click the device name to display the Interfaces list. Click **Devices Home** to return to the main **Devices** page.
3. Click the **Assets** tab. Grid Manager displays all assets associated with the chosen device.

Copyright ©2019, Infoblox, Inc. All right reserved.
Grid Manager displays the following information for each asset:

- **Name**: The asset name on the network as discovered by Grid Manager. If the name is that for another infrastructure device, you may click on it to see its associated assets.
- **Interface Name**: The name of the interface (usually a switched interface) associated with the discovered device.
- **VRF Name**: The name of the VRF associated with the interface, if applicable.
- **Network View**: The name of the network view to which the VRF instance belongs, if applicable. If there is only one network view in the Grid, which is the default view, the Network View column is hidden by default.
- **VRF Description**: The description about the VRF instance, if applicable.
- **IP Address**: The IP Address for each discovered asset as managed by NIOS and IPAM. The IP address is a link to the home IPAM page for the interface.
- **Type**: The type of device. Infrastructure devices such as routers and switches may also be categorized as an Asset.
- **Username**: The Username for the asset, as defined from the host's DHCP lease.
- **Asset MAC Address**: The hardware MAC address associated with the asset.
- **VLAN Name/VLAN ID**: The VLAN identifier from which the asset is reachable.
- **Admin Status**: The administrative status (Up or Down) of the management port that identifies the asset device.
- **Operation Status**: Normally reads Up or Down. Asset records may appear as Down because they are disconnected from the network or being rebooted.
- **Managed**: Indicates whether the asset is managed by NIOS.
- **Reservation**: Indicates whether the interface has a port reservation bound to it.
- **Capabilities**: Describes the capabilities of each interface in the selected device. Hover the mouse over each entry to view the complete listing.
- **Site**: This is a predefined extensible attribute.

Using the Action icon

- you can perform the following tasks in the IP Addresses page:
  - **Edit IPAM Object**: For managed objects, this opens the editor for the object so you can modify its properties.
  - **Edit Interface**: Opens the interface general settings page. You can view and modify basic interface settings such as Admin Status (on the General page), Data VLAN and Voice VLAN (on the VLAN page), and add or modify extensible attributes.
  - **Show IPAM IP Address**: Shows discovered data, related objects, and audit history of the selected asset. This option is disabled for devices that have a management IP that is not part of an IPAM network. Discovered data may or may not appear for the asset, depending on the device type.
  - **Convert**: Depending on the asset type and its IPAM status, you may be able to convert the selected asset to a Host Record, A Record, PTR Record or a Fixed Address. Otherwise, Grid Manager shows **This object cannot be converted**. You can also perform the same action by selecting an IP address check box and clicking **Convert** from the Toolbar.
  - **Device Details**: Provides information about the device to which the selected IP address belongs. The list includes information such as the IP Address and Device Type for the device, and in the IPAM Type field whether the device itself is a managed or unmanaged object in NIOS. It also provides the following status counters for the device:
    - **Total Available Interfaces**: The total number of interfaces associated with the device.
    - **Administrative Up - Operational Up**: The number of ports that are fully up and passing traffic.
    - **Administrative Up - Operations Down**: The number of ports that are administratively up, but have some kind of connectivity issues.
    - **Administrative Down - Operational Down**: The number of ports that are administratively taken down.

**Viewing Assets Associated with an Interface**

You can narrow down an Asset list to individual interfaces on any managed network device. On the interface level, the Assets page shows all devices associated with the chosen interface, including switchports supporting many end hosts. In practice, most Asset tables show end hosts and devices that populate Ethernet network segments.

1. From the **Data Management** tab, select the **Devices** tab.
2. Click the **Name** link for the device you want to inspect.
3. Click the Action icon

for an interface in the table, and choose **Show Assets**. (Applies only to switched interfaces that do not have an IP address.)

Values listed in the Assets table include the following:

- **Name**: The asset's name on the network as discovered by Grid Manager. If the Name is that for another infrastructure device, you may click on it to see its associated Assets.
- **Interface Name**: The name of the interface (typically a switched interface) associated with the asset (by which the asset was discovered).
- **IP Address**: The IP Address for each discovered end host as managed by IPAM. The IP address is a link to the home IPAM page for the interface.
- **MAC Address**: The hardware MAC address associated with the asset.
• **VLAN ID/VLAN Name**: The VLAN identifier from which the asset is reachable.
• **Operation Status**: Normally reads **Up** or **Down**. Asset records may appear as **Down** because they are disconnected from the network or being rebooted.

In the Interfaces page, if you select an interface for a switch that is only connected to a neighboring switch, router, or switch-router, and then choose **Show Assets**, the Assets page displays only the neighboring device that is reachable from the chosen port.

### Viewing Components of Discovered and Managed Devices

Network Insight provides a table of hardware components for each discovered/managed network device. Elements listed in the Components table include the following:

• **Name**: The discovered name of the device component.
• **Description**: The description string associated with the component. In many cases, this value is the same as the Name field.
• **Class**: Type of component. Possible values include, but are not limited to, Port, Power Supply, Fan, Module, Stack, RoutingEngine, powerEntryModule, Chassis, and more, based upon the collected SNMP data.
• **Serial Number**: The discovered vendor serial number for the component.
• **Model**: Describes the model number or model name of the component, based upon collected SNMP data.

**Note**: Click Device Details in the Toolbar to view information about the device, including its IPAM Type and the operating status of its ports.

### Viewing Discovery Status

**Note**: Opening Discovery Status for viewing requires Superuser permissions under Grid Manager.

You can view a list showing the complete Discovery status of all device or of selected devices.

To isolate devices for evaluation, use filtering to reduce the list. Click **Use Filter** at the top of the table and choose **IP Address**, **Name** or **Overall Status** as the filter.

1. From the **Data Management** tab, select the **IPAM** tab. The IPAM Home page appears.
2. Expand the Toolbar and click **Discovery Status**. The same **Discovery Status** button can be found under **Data Management → Devices**.

The Discovery Status table lists detailed information about network devices and end hosts discovered through all methods, including SNMP, ICMP ping sweeps and other processes.

- **IP Address**: the IPv4 or IPv6 address of the discovered device. You can filter the table by this value.
- **Name**: The name of the discovered device as reported through SNMP. You can filter the table by this value.
- **Type**: The discovered device type. Examples include **Router**, **NIOS**, **Switch-Router**, **Firewall**, **Load Balancer**, and numerous others.
- **Overall Status**: Indicates the overall success or failure of the discovery task on the device. Hover the mouse over the device to see more detailed information about the discovery status, including the timestamp of the last discovery event, confirmation of detection ("Device Exists"), and the means of detection, which are usually methods such as SNMP, reading the ARP table or location through a Seed router. You can filter the table by this value.
- **Reached Status**: Indicates the reachability of the discovered device. Typically, devices are reported **Passed** for Reached Status if they are reachable through SNMP, a path trace through ICMP, or UDP-based path tracing for an IPv6 address. You may see a **Reached Status of Passed** and still receive an **Overall Status of Failed**. This often occurs because either the CLI credentials or SNMP credentials provided for discovering the device do not work, or another problem occurs in some part of the discovery process.
- **SNMP Collection Enabled**: Indicates whether the managed device allows SNMP as a management protocol. This value shows **Yes** or **No**. You do not see any SNMP collection status updates if this value shows No.
- **SNMP Credential Status**: Indicates whether the correct SNMP credential is used by discovery. Usually shows simple **Passed** or **Failed** status. Passing the mouse over the Failed status reading for this column shows the location in the SNMP data collection where information gathering failed. The typical message for a failure of this type typically shows Failure to Authenticate, which simply means that the correct SNMP credentials have not been provided for either SNMPv1, SNMPv2c or SNMPv3 as required and defined for the device's discovery configuration.

If **SNMP Credential Status** shows Failed, you do not see a value under **SNMP Collection Status**, because that is dependent on successful credential authentication. Should you succeed in SNMP Credential Authentication for a device, this value shows **Passed**.

- **SNMP Collection Status**: Indicates whether managed device information has been successfully collected from the device. If the current device shows an **SNMP Collection Status** of Failed, this field remains blank. Should you succeed in SNMP Credential Authentication, **SNMP Collection Status** may or may not show a Passed outcome. If the final outcome is successful, passing the mouse over the table value shows the SNMP data set that was successfully collected from the device. When the **SNMP Collection Status** is set to **Passed**, it indicates that the credentials provided in **Member Discovery Properties** for discovering the device are correct and discovery has completed successfully on the device. For more information, see **Defining the Discovery Member Type**.
• **CLI Credential Status:** Reports the basic success state of CLI credential usage for device discovery. When you see a Failed status in this column, hover the mouse over the table value. Details related to failed CLI credentials normally relate to “Failed to Authenticate” events. (For more information, see the following subsection Analyzing Discovery Status.) If you define device discovery requirements to use both SNMP and CLI, and you receive complete SNMP discovery information but fail to authenticate for CLI, the **Overall Status** for the device remains as **Failed**.

• **CLI Collection Enabled:** indicates the CLI collection configuration state for the discovered or managed device. Possible values are **Yes** (CLI collection is enabled) or **No** (CLI collection is disabled for the device).

• **Fingerprint Status:** Shows the status of discovery of the device's OS through fingerprinting.

• **Last Update:** Timestamp showing the conclusion of the last data update for the current device.

• **First Seen:** Timestamp showing the initial discovery event.

• **Last Seen:** The date and time when the device was last successfully polled by discovery.

• **Last Action:** The last action performed by discovery upon the device after the discovery took place. Hover the mouse over this field to obtain details.

Visible columns can be changed in the Discovery Status window. At the top of any column header, click the down arrow tool, and choose **Columns – > Edit Columns**.

### Analyzing Discovery Status

When you see a status of Failed for a device under **Overall Status**, the problem usually relates to issues in discovery data collection. When **Overall Status** shows a value of **Passed**, it indicates that everything has passed for the device. If the value is **Failed**, it indicates that one or more elements of the device have failed discovery. Your discovery settings have a great deal to do with what you see in the respective Status columns. You key on the Overall Status result and read columns to the right to narrow down possible causes. To start, you typically see three basic discovery credential configurations for network devices:

- SNMP credentials and no CLI credentials;
- SNMP credentials and CLI credentials;
- No SNMP credentials, CLI credentials only.

Begin by considering SNMP-only device discovery configurations. In the table, **Overall Status** shows only a simple Failed message with no detail. Go to the next data column, which is **Reached Status**. If the device proves reachable, this value shows Passed, indicating that discovery can successfully reach and query the device. If **Reached Status** shows Failed, this is the first and most fundamental problem, that the device cannot be Pinged or contacted in any way across the network.

As an example, assume a **Reached Status** value of Passed. If the device is reachable, discovery can successfully attempt SNMP or CLI communication to the device. Beginning with SNMP, and assuming that SNMP collection is enabled, select the **SNMP Credential Status** counter. If it shows Failed, that normally indicates a Failure to Authenticate, which can be shown as a tooltip by hovering the mouse over the table field:

A successful **SNMP Authentication** may or may not result in successful data collection:

![SNMP Authentication Success](image1)

A successful authentication also shows which protocol was used for SNMP authentication; SNMPv1, SNMPv2c or SNMPv3. This does not guarantee successful data collection through SNMP, however. The **SNMP Collection Status** counter shows possible Passed and Failed values. Hovering the mouse over a Failed value in this column shows a tooltip reporting the set of data that discovery could not collect through SNMP. When discovery encounters an error during collection of a specific data set (Forwarding table, or System identification data, for example), data collection stops and issues an error message and an SNMP trap, which is reported and also appears in the tooltip. If **SNMP Collection Status** shows a value of Passed, and discovery does not use CLI data collection on the device, discovery has successfully completed on the device.

The **CLI Credential Status** counter also reports either Passed or Failed results, and uses tooltips to tell the user what is going on in more detail.

![CLI Credential Status](image2)

CLI credentials failure messages are straightforward and can be tested by verifying login tuples or Enable passwords from the credential sets defined in discovery configuration.

If you receive a **CLI Credential Status** value of Passed, the correct command-line admin login information is specified in the discovery configuration.
configuration.
For more information about checking and diagnosing discovery behavior for devices listed in the status table, see the following topic Executing Discovery Diagnostics.

Executing Discovery Diagnostics

You can execute a discovery diagnostic to help determine why a specific device is presenting difficulties in discovery. For example, a given device may be reachable but show an overall status of Failed in the Discovery Status dialog. A discovery diagnostic steps through a complete discovery process based on the configuration on the Probe member to which the device is assigned. The diagnostic runs the gamut from fetching SNMP object ID information to ARP table reading and to ICMP pings and traceroutes.

You can do the following in the Discovery Diagnostics dialog:

- View all existing discovery diagnostic tasks that were executed in the last 12 hours.
- Enable or disable SNMP debugging for a device. The SNMP debugging is enabled by default.

Note that you must be a superuser to perform a discovery diagnostic. To execute a discovery diagnostic, complete the following:

1. From the DataManagement tab, select the IPAM tab, and then click DiscoveryDiagnostics from the Toolbar.
2. In the Discovery Diagnostic editor, complete the following:
   - Existing Discovery Diagnostic Task: Select this option to choose an existing discovery task from the drop-down list. The appliance displays all the discovery diagnostic tasks that were executed in the last 12 hours in the drop-down list.
   - New Discovery Diagnostic Task: Select this option to initiate a new discovery diagnostic. To start a new discovery diagnostic task, complete the following:
     - IP address: Enter the IPv4 or IPv6 address of the device on which you want to perform the test. The discovery diagnostic runs a full discovery procedure against the specified IP address. Ensure that you select the respective network view in which this IP address resides.
     - NetworkView: If you have multiple network views, select the network view in which the IP address resides from the drop-down list. If you have only one network view, which is the default view, the NetworkView drop-down list is hidden by default. NIOS conducts a discovery diagnostic for the IP address in the selected network view.
     - CommunityString: Specify the community string for the device if the required SNMP credential is not currently configured for the discovery member. It may not be necessary to enter a community string if the device is already discovered by NIOS and is a managed device.
     - ForceTest: To force a diagnostic against the device, select Yes.
   - Enable SNMP debug: As a troubleshooting aid, the SNMP debugging option is enabled by default. When you enable this option, the appliance collects all SNMP communications between NetMRI and a device. The SNMP logs are useful for troubleshooting purposes. Clear this check box to disable the SNMP debugging for a device.
3. Click Start to start the discovery diagnostic. The lower pane displays the complete discovery sequence for the chosen device, and whether or not the discovery is successful. You can click Stop at any time to end the diagnostic sequence.

The output log of the diagnostic is displayed in the lower pane, and it shows the attempt for the complete discovery process. You can then do the following:

- You can click Select All to select the complete text in the lower pane for copying and pasting to the Clipboard and a text editor. You can also monitor the test messages in this pane.
- Click Download as text to download the complete discovery diagnostics in a text file for the selected device. The default name of the downloaded file is discovery_diagnostics_nnn.nnn.nnn.nnn.txt, where nnn.nnn.nnn.nnn is the IP address of the selected device. The Dow nload as text button remains disabled until the download is complete.

Viewing the Management State of IPs in Discovered Networks

You can view the management state for any IP address, in any network, that is associated with any discovered device.

1. From the Data Management tab, select the Devices tab. The Devices Home page displays a list of all devices currently found and catalogued by discovery.
2. Click the Action icon
   for a chosen device and choose Networks from the popup menu.
3. Choose a network from the list. Grid Manager switches to the IPAM page view of the selected network.
   The IPAM Home page displays the IP Map for the chosen network. The page shows information in graphical format, indicating elements such as Used Addresses, fixed addresses and IP reservations, Unmanaged IPs, Host Not in DNS/DHCP, and all other objects or information associated with IP management. The user benefits from this view by immediately seeing which IPs in the network contain devices that remain unmanaged by Grid Manager. These Unmanaged IP values appear in light yellow. Hovering the mouse over any IP address in the graphical table shows the information that has already been determined about the IP address.

Note: An Unmanaged IP cannot be converted to Managed unless the network that contains it, is converted to managed status. For more information, see Converting Unmanaged Networks under IPAM to Managed Status.
Disabling Discovery for a Network

You go to the DHCP feature under **Data Management** to disable discovery for a network. Disabling discovery for a network differs from discovery blackouts; disabling discovery for a network simply ensures that discovery never takes place on the chosen network.

To disable discovery for an IP network:

1. Select a managed network from one of the following locations:
   a. **Data Management** → **IPAM** → list view
   b. **Data Management** → **DHCP** → **Networks**
2. Click the Action icon next to the network you want (this automatically selects it) and select **Edit** from the menu. The Network editor appears.
3. Click the **Discovery** tab.
4. Child networks inherit their discovery default settings from their parent networks. Click **Override** to change the **Enable Discovery** setting. (The **Discovery Member** setting remains unchanged.)
5. Deselect the **Enable Discovery** check box, and then save the configuration.

Adding Discovery Device Support

**Note:** Adding Device Support Bundles, viewing and deleting them requires Superuser permissions.

Infoblox frequently provides support files for additional network devices that may not previously be supported by discovery, and updates to support new operating system versions of existing devices. To add device support updates:

1. From the **Grid** tab, select the **Device Support** tab.
2. Expand the Toolbar and click **Add**.
3. Click **Select** and navigate to the file you want to upload.
4. Select the file, and then click **Upload**.

   The Device Support table shows its installed library of files with the following data points:

   - **Name**: The descriptive device name for the device support file.
   - **Version**: The version of the currently active device support file.
   - **Author**: The developer of the device support file.
   - **Type**: The Type column lists two types of Device Support files: the System type indicates a support bundle that is installed with the NIOS/Grid Manager system. The Downloaded type indicates device support bundles that are installed by the administrator. System bundles are read-only and cannot be removed or overwritten by administrators.

You may remove custom support bundles that you have installed on the Device Support Page. To do so, click the Action icon for a chosen device and choose **Delete** from the popup menu.

Port Control Features in Network Insight

**Note:** Port control involves two primary operations: *network provisioning/de-provisioning* and *port configurations*. These operations are classified as port control tasks that can be monitored and viewed in the Task Manager (**Administration** → **Workflow** → **Task Manager**).

Port control enables changes to the interface-level configurations of switches and switch-router devices, and assignment of these resources to network objects defined and created within IPAM.

- Port configurations and network provisioning and de-provisioning use CLI admin credentials, supporting SSH and Telnet. You may test credentials before use, against an IP address or a selected device;
- Port configuration consists of two primary operations: setting admin status for a port, and defining Data VLAN and Voice VLAN assignments (where applicable), along with minor changes such as editing descriptions;
- You can define port configuration blackout periods using the same methods provided for discovery blackouts. These blackout periods also apply to network provisioning and de-provisioning tasks;
- Configuring a port on a device always creates a new port control task that can be viewed and managed in the Task Manager.
- You can separately schedule port control tasks using the same method as for object creation.
- You can edit interfaces, inline, from the **Interfaces**, **IP Addresses** and **Assets** pages in Grid Manager. These operations generally consist of setting the interface to be Administratively Up or administratively Down, and VLAN assignments (see **Inline Interface Editing**);

Network provisioning includes the following:

- If a user deletes a discovered network from the system, Grid Manager displays the list of interfaces on which the network is currently provisioned;
- Network provisioning allows you to provision a network on one interface at a time. The network must be in managed status under IPAM;
- The user can also *de-provision* a network, which removes it from one or more interfaces;
- You can perform network provisioning and de-provisioning tasks on routers and switch-routers.

Devices do not have to be in managed state for some port control operations (setting ports to Admin Up and Admin Down, for example) but some port control operations require it.
• Provisioning a network (through IPAM) onto a port on a managed device;
• De-provisioning a network.

When you create a new object using the wizard, you can configure the port or ports that are associated with the object's port reservation. In this case, two new tasks are created: an object creation task, and a port control task, which can be scheduled separately from the object creation. The port control task is a separate task that may also require administrator approval. When you create a new task, an information feedback panel provides a link to the port control task in the Task Manager. You may also select and reschedule both tasks. For more information, see Rescheduling Tasks.

Note: If you edit an object, you can only edit an associated port reservation.

Objects are completed in their configuration by Grid Manager before executing a port configuration. If, for example, a fixed address object is subject to administrative approval, no port control task takes place for that object until the approval is executed and the object is created. This has implications for scheduling: if you schedule the creation of a new host, IPv4 reservation or fixed address, and wish to schedule a port control task for the same object, the scheduled object creation must take place first, and must complete, before the scheduled port configuration executes.

All port configuration operations can be scheduled and subject to administrator approval. For more information, see Configuring Approval Workflows.

About Port Reservations

You can define a device port reservation for a defined object such as a host, fixed address or IPv4 reservation, or for an Infoblox Grid Member. Port reservations assign device interfaces to Infoblox-managed objects in Grid Manager. The port reservation is a property of each object, such as a fixed address or host record, that you create.

After discovering and cataloging infrastructure and devices, Grid Manager compiles the lists of interfaces and separately tracks available switch ports on each device. When you attempt to reserve a switch port, Grid Manager provides the complete list of available switch ports on the device, automatically preventing possible conflicts over port usage.

Characteristics of port reservations include the following:

• Device Ports can be reserved to Grid Manager objects under IPAM and DHCP;
• The user can choose to immediately create the new object (IPv4 reservation, IPv4/IPv6 fixed address or host, or a Grid member), and to also immediately assign a device port to the object. In such cases, the object is created and the port is reserved for the object;
• An object can be scheduled for creation at a later time, and its port assignment scheduled for the same time, or for a different date and time, in the future;
• A port reservation does not guarantee that the switch interface is in fact available for the assignment.

• You can create port reservations for multiple objects at a time;
• Interface tables show the objects to which they are bound, in a special Reservation column;
• When you delete an IPAM object such as a fixed address, its associated port reservation is automatically deleted.

Once a switch port or other device port is reserved, Network Insight prevents future tasks from trying to use the same port for another reservation. Device switchports and router interfaces, and other interface types may be assigned to the following types of objects:

• Grid members (including HA Pairs). For more information, see the following sections Defining Port Reservations for an Infoblox Grid Member and Defining Port Reservations for an HA Pair.
• Hosts. For more information about defining hosts with included port configuration, see Adding Host Records.
• IPv4 reservations. For more information, see Adding IPv4 Reservations.
• Fixed addresses (IPv4 and IPv6). For more information, see Adding IPv4 Fixed Addresses and Adding IPv6 Fixed Addresses.
• IP networks (IPv4 and IPv6). For more information, see Adding IPv4 Networks and Adding IPv6 Networks.

Devices involved in these operations must be under managed status in Grid Manager. For more information, see Converting Unmanaged Devices to Managed Devices.

Editing Interfaces in a Device

Note: Voice VLAN settings are applicable only for Cisco devices.

To speed port configuration workflows, you can select one interface or multiple interfaces for a device to change the admin status, description and VLAN settings. For example, this feature is handy if you want multiple interfaces to participate in the same data VLAN. There are two ways to approach this feature: directly from the Devices page, or by selecting a device on the Devices page, opening its Interfaces page and selecting ports from there.

Editing interfaces is done from the main Data Management --> Devices page.

1. From the Data Management tab, select the Devices tab.
2. Click the Action icon
   🛠 for a chosen device and choose Interfaces from the popup menu.
3. Select the check box for a specific interface, click the Action icon

Copyright ©2019, Infoblox, Inc. All right reserved.
for the interface and choose **Edit**. The interface editor appears as shown in **Figure 15.12**.

**Figure 15.10 Interface Editor, with editable Admin Status and Description settings**

4. The editable settings are **Admin Status (Up or Down)** and **Description** (click inside the field to edit). In some cases, owing to device permissions, the device type or other device settings, you may not be able to edit these values for the selected interface.

5. To edit VLANs for the chosen interface, click the **VLAN** tab. **Figure 15.12** shows an example. VLAN editing also is subject to permission limitations based on the device, and on the device type.

**Figure 15.11 Editing VLANs**

6. Choose a data VLAN to assign to the port from the **Data VLAN** drop-down menu.

7. If supported, choose a voice VLAN (Cisco only) from the **Voice VLAN** drop-down menu.

8. Click the **Extensible Attributes** tab to add any attributes that are necessary for the interface.

9. Click **Save & Close** to close the interface editor.

**Editing Multiple Interfaces**
To edit multiple interfaces for a device:

1. From the Data Management tab, select the Devices tab.
2. Click the Action icon for a chosen device and choose Interfaces from the popup menu.
3. Select the check boxes for each interface that you want to edit.
4. Expand the Toolbar and click Edit. The Interfaces editor appears as shown in Figure 15.12.

   **Figure 15.12 Editing Multiple Interfaces**

You can select one or more interfaces for configuration, define their settings in the dialog, and then select other interfaces and define different settings for them.

**Note:** Once you change Admin Status, Data VLAN or Voice VLAN settings for any selected port, no automatic eversion exists to the original settings from the same editing session. You must cancel out of the Interfaces editor to reject any changes and begin with a new editing session from the Interfaces page. Use the Verify button to verify your changes.

5. Select the check boxes for one or more ports and define the Port Configuration settings for the following:
   
   a. Admin Status: Select Up or Down from the menu, depending on the current state of the port(s);
   b. Description: Provide a brief description of the port configuration or other information;
   c. Data VLAN: (Hidden if editing a VLAN is not supported) Drop-down list of all data VLANs actively configured in the current device. One of the values can be chosen for the currently select interface(s);
   d. Voice VLAN: (Hidden if editing a voice VLAN is not supported) Drop-down list of all voice VLANs actively configured in the current device. One of the values can be chosen for the currently select interface(s).

6. After making configuration changes to all ports, click Verify to check over your changes:

   **Figure 15.13 Verifying port configuration changes**

7. Click OK. The changes are not committed by doing so.
8. If the port configuration changes are correct, click Save & Close or click the Scheduling icon at the top of the editor. To schedule this task, click the Schedule icon at the top of the editor. In the Schedule Change panel, click Later, and then specify a date, time, and time zone. The Schedule icon is green when there is a pending scheduled task. You can reschedule the task if you have the applicable permissions.

When you complete the configuration, all port configurations in the session are combined into a single task by Grid Manager.

Editing Multiple Interfaces from the Devices Page

The Data Management → Devices page allows you to immediately set the Admin Status, descriptions and VLAN settings for any selection of ports on a single device.

1. Click the Action icon for a chosen device and choose Edit from the popup menu. The Interfaces page appears for the device editor.

2. Select the check boxes for one or more ports and define the Port Configuration settings for the following:
   a. Admin Status: Select Up or Down from the menu, depending on the current state of the port(s);
   b. Description: Provide a brief description of the port configuration or other information;
   c. Data VLAN: (Hidden if editing a VLAN is not supported) Drop-down list of all data VLANs actively configured in the current device. One of the values can be chosen for the currently select interface(s);
   d. Voice VLAN: (Hidden if editing a voice VLAN is not supported) Drop-down list of all voice VLANs actively configured in the current device. One of the values can be chosen for the currently select interface(s).

3. After making configuration changes to all ports, click Verify to check over your changes.
4. Click OK. The changes are not committed by doing so.
5. If the port configuration changes are correct, click Save & Close or click the Scheduling icon at the top of the editor. To schedule this task, click the Schedule icon at the top of the editor. In the Schedule Change panel, click Later, and then specify a date, time, and time zone. The Schedule icon is green when there is a pending scheduled task. You can reschedule the task if you have the applicable permissions.

When you complete the configuration, Network Insight combines all port configurations in the session into a single task.

Inline Interface Editing

You can directly edit a device's interface listings in the Interfaces page. Double-click any table row and the fields that you can edit for the row, which consist of the VLAN ID, Admin Status and Description fields for each interface, open in an inline editing selection field. Fields are editable as applicable to device types. If you are editing an interface on a L2 switch, for example, the VLAN ID field does not appear.

Figure 15.14 Editing Interface values inline.

Double-clicking a table row opens the editable fields for the selected record. If editable fields are not present in the table display, you cannot change their values in the Interfaces page. After making inline changes, click Save on the selected row to commit them. To prevent using any changes, click Cancel. This also de-selects the row.

Note: When you make inline changes to an interface, a new task is created under Grid Manager, which you can view in the Task Manager page (for more information, see Viewing Tasks). A status icon appears next to the interface element you have changed, indicating the status of the new task and providing a link to the Task Manager page. New tasks appear with a status icon of Pending (||). When the new task completes, the icon changes to a green checkmark.

Provisioning and De-Provisioning Networks

Copyright ©2019, Infoblox, Inc. All right reserved.
You may provision networks and remove or de-provision networks from individual devices. You can also provision networks when creating a network in IPAM (for more information, see Adding IPv4 and IPv6 Network Containers and Networks). Network provisioning and de-provisioning comprises the second type of port control tasks under Network Insight. Provisioning a network involves creating a new network and adding it to the list of networks in IPAM, and also involves changes to device configuration.

**Note:** If a port control task requires administrative approval, and it is not approved before its scheduled execution, the task appears as unsuccessful in Task Manager.

Provisioning networks also allows for provisioning VLANs. If devices do not support VLANs, options for provisioning VLANs do not appear for those devices and their associated interfaces.

If a network is already provisioned for an interface, regardless of its status under Grid Manager, you cannot provision another network upon it.

Only available interfaces that support network provisioning are shown in Grid Manager for provisioning tasks. The horizontal toolbar also provides related functions:

**Provision Network**

: Available for discovered devices and for managed devices, this icon opens the Provision Network feature, allowing you to provision an existing IPAM network onto the selected device by selecting a device interface or assigning a VLAN. Grid Manager creates a new Port Control task, and you can choose the interface on which the network is provisioned, along with VLAN configuration and other settings.

**De-provision Network**

: Available for networks that are managed under IPAM, for de-provisioning on devices that are managed under IPAM on the Data Management – Devices page. A dialog box appears summarizing the task you are instructing Grid Manager to perform. This action changes the configuration of the device.

To provision IPAM networks onto a device:

1. From the Data Management tab, select the Devices tab.
2. Click the Next Page and Last Page icons to locate the device whose interfaces you want to provision.
3. Click the Name of the device. The Devices page displays the five tabs of information associated with the device.
4. Click the Networks tab.
5. The Networks page lists all discovered networks (highlighted in grey), unmanaged networks (highlighted in yellow), and any managed networks (highlighted in white, showing Yes in the Managed column) present on the selected device.
6. Open the vertical toolbar and click Provision Network. The Provision network wizard appears.
7. Click Select Network to choose the network the you want to provision. If only one managed network is available on the device, that network value is populated after clicking the button.
8. Choose the network to provision onto the device and click OK.
9. Enter the Router IP Address. This required field may be pre-populated with the DHCP router IP address if the device already has a DHCP configuration. If not, enter the gateway router IP address for the current device.
10. If necessary, check the DHCP Forwarding check box. Check this check box to enable DHCP forwarding for the newly provisioned network. If a DHCP failover is already present, the IP addresses from that failover are used for DHCP forwarding information.
11. For choosing the Interface, you can choose one out of two options:
   a. **Interface** drop down list: If you are provisioning the network directly onto an interface, select it from this list. Only interfaces that are available for provisioning on the chosen device appears on this list; interfaces that are already active in a network do not appear;
   b. For a switch-router, select Create VLAN, and specify the VLAN Name and its new VLAN ID. Ensure that the VLAN ID is not one that is already provisioned on the device.

**Figure 15.15 Provisioning a VLAN on a Switch-Router**

![Provisioning a VLAN on a Switch-Router](image)
De-provisioning Networks

Note: De-provisioning a network changes the device configuration. As such, a separate task is created for the action under Task Manager. However, you cannot schedule the de-provisioning of a network—once you confirm the de-provisioning action in Grid Manager, the action takes place. Each managed and unmanaged device under Grid Manager provides a Permissions page (Data Management -> Devices -> Select Device -> click Edit -> Permissions tab). By default, no admin group or Role is assigned to managed devices. Infoblox recommends using caution when assigning rights to users that may be able to access devices and change device configurations.

De-provisioning networks is a relatively straightforward task that can be performed for any selected network, whether it is a non-NIOS network (a network that cannot be configured in IPAM), an unmanaged network, or a managed network.

Note: If the network is also managed under IPAM, de-provisioning the network from a device does not delete the network from IPAM.

If you are deleting a network from the main IPAM page, any devices that have endpoints provisioned on that network are also de-provisioned for that network.

Note: A network may not be de-provisioned until after you set the interface for the network on the device(s), to Down in Admin Status.

1. From the Data Management tab, select the Devices tab.
2. Click the Next Page and Last Page icons to locate the device through which you want to locate the interfaces to convert.
3. Click the Name of the device. The Devices page displays the five tabs of information associated with the device.
4. Click the Networks tab for the chosen device. The Network page lists all discovered networks (highlighted in grey), unmanaged networks (highlighted in yellow), and managed networks (highlighted in white) present on the selected device.
5. Click the Next Page and Last Page icons to locate the network that you wish to de-provision.
6. Click the Action icon next to the network you want (this automatically selects it) and select De-Provision Network. The dialog box appears, listing the device name, the device's IP address, the interface to which the network is currently bound, and the network's endpoint IP address on the current device.

Figure 15.16 De-Provisioning a Network from a Device

![De-Provisioning a Network from a Device](image)

Note: Ensure that the de-provisioning of the network has administrative approval.

You can also select multiple network entries from the list on the same device and de-provision all of them in a single step. Exercise caution when performing such actions.

De-Provisioning Networks by Deleting Networks in IPAM

Note: Deleting a network under IPAM creates a new Object Change task in Task Manager. You can check the Administration -> Workflow -> Task Manager page to view its status.

You can simply delete a managed or unmanaged network in IPAM to de-provision it. Doing so opens a Delete Confirmation dialog. IPAM also automatically prompts you to verify that you are deleting the network from all devices that have interfaces connecting to the network, subject to verification and permissions.

By default, when you delete the network, all devices that connect to the network, that are also managed by IPAM, are part of the new
Troubleshooting Port Control Tasks

Issues can occur when attempting to define port configurations on devices. When you define port configurations through Network Insight, you are defining a port control task that can be viewed, investigated, and run again when necessary. You do so by using the Task Manager (Administrati

on → Workflow → Task Manager) and looking for tasks that show a Type of Port Control. Each Port Control task provides an Execution Log and the ability to re-run a task that has failed for any reason.

The Task Manager page provides an Action icon column with a series of menu options for features related to Grid Manager tasks to manage task execution, scheduling and approval. Menu choices change based upon the context and the current state of tasks in the table; features available in the Action menu include the following:

- **Approve**: Enables admins to approve a pending job.
- **Reject**: Enables admins to reject a pending job, immediately cancelling it.
- **Execution Log**: Opens a completed task’s execution log window. The Execution Log lists the complete communications sequence sent to a device to perform a port control task.
- **Execute Now**: Force a selected pending task to execute immediately.
- **Re-Execute**: Allows you to re-run the selected task. Combined with the Execution Log, this process can aid in troubleshooting a failed port control task.
- **Reschedule**: Opens the Reschedule window for the selected task. To immediately execute this task, click Now. Or, in the Reschedule panel, click Later, and then specify a date, time, and time zone. You can reschedule the task if you have the applicable permissions. Click Save to commit the changes.
- **Delete**: Deletes the pending task.
- **View**: Opens the Task Viewer to the currently selected task.

The Execution Log allows you to see task behavior when it executes. You can check the configuration directly on the device and re-run the job if it has failed, by selecting Re-execute from the Action menu on the Task Manager page.

Creating Port Reservations for IPAM Objects

A port reservation instructs Network Insight to reserve ports on discovered and managed devices, for exclusive use by Grid members and by IPAM objects such as hosts or fixed addresses. Network Insight ensures that doing so does not interfere with existing device and port configurations and active networks, because port reservations automatically apply only to ports that are discovered to be available on network devices. Network Insight prevents a user from reserving the same port for more than one object. Should a port reservation somehow conflict with another more recent port reservation, Network Insight automatically reports a conflict and enables you to respond to the issue (for more information on this topic, see Resolving Port Reservation Conflicts).

When you create new IPAM objects, you can create the new objects and define port reservation settings at that time, or create the new object without any port-related settings and edit them later, after the object is established in Grid Manager. The Add IPv4 Reservation Wizard, Add Fixed Address Wizard, Add Host Wizard and Add Grid Member Wizards all support the full set of port configuration settings, as shown in Figure 15.18. Defining Port Reservations during Object Creation.

Making a port reservation does not guarantee that the port is in fact available on the requested device. All interfaces appearing in the Interface list...
are ports that are otherwise known to Network Insight as Operationally Down during its last discovery task, and that are not already reserved by a port reservation.

1. Begin by checking the Reserve Port check box.

   **Note:** Optionally, you can completely skip port reservation and port configuration by clicking **Next**.

2. Click the Device Name button to choose the device for which the port reservation is associated. You should know the identity of the device to which the Infoblox appliance is connected before taking this step.

3. After choosing the device, choose the Interface with which the reservation is bound. The drop-down list shows only interfaces that are most recently found to be available by Network Insight during the last discovery cycle. This list does not include any ports that are Administratively Up and Operationally Up and are otherwise already assigned to other networks or objects.

   - The Wizard page also shows a list of any VLANs that are currently configured in the chosen device. This Wizard page does not allow the definition of new VLANs for port configuration—only the assignment of an existing VLAN in the device for port configuration.

4. Select the Configure Port check box to define specific port control settings for the port reservation.

   **Note:** If you do not take this action when you create the object, you cannot perform the configuration later while editing the object.

5. If the chosen device supports them, choose the Voice VLAN and/or the Data VLAN settings you may need for the port assignment. You do not create new VLAN values in this step; you can select from VLANs that are provisioned on the currently chosen device. All VLANs configured on the device and discovered by Network Insight during its most recent discovery polling cycle appear in the drop-down lists.

6. Set the Admin Status to Up if you need to activate the port in the current task. Though the port reservation is associated only with the current object, any port configuration creates a new Port Control task under Task Manager.

7. Enter a Description for the port assignment. Infoblox recommends doing so to help other technicians to recognize the port assignment event.

8. When finished, click Save and Close or select other tabs to change settings for the object.

   **Note:** Once a switch port or other device port is reserved, Network Insight prevents further port reservations from using the same port for another reservation.

See the following sections for examples on how to create IPAM objects with port reservations:

- Adding Host Records
- Configuring IPv4 Networks
- Configuring IPv4 Fixed Addresses
- Configuring IPv4 Reservations
- Configuring IPv6 Networks
- Configuring IPv6 Fixed Addresses
- Adding Grid Members
- Defining Port Reservations for an Infoblox Grid Member

**Editing Port Reservation Settings for IPAM Objects**

As previously noted, you can create IPAM objects such as hosts or fixed addresses without device information and port reservation settings, and edit them later after the object is established in the Grid Manager. You can change port reservations in any object to new settings. Limitations exist when editing existing objects.

The **Port Reservation** editing page settings uniformly apply to Grid members, IPv4 reservations, hosts, and fixed address objects. Note that you cannot change port configurations when editing objects, as shown in *Figure 15.19*.

*Figure 15.19 Editing an Existing Object's Port Reservation*
Unlike creating an object, editing an existing object's port reservation does not permit configuring the selected port. (You can edit the port from the device's Interfaces page, including inline editing.) Physical interfaces with an Operational Status of Down appear in the Interface drop-down list. Ports that are already active, that are reserved through a port reservation, or that are administratively Up/Operationally Up do not appear in the Interface drop-down list.

For object editing, you can select interfaces but you cannot edit their settings, such as setting the Admin Status to Up or choosing the Data VLAN or Voice VLAN.

Port reservation editable settings are as follows:

- **Reserve Port**—Enables the port reservation task for the new object;
- **Device Name**—Shows the name of the chosen devices, which must be selected by clicking Select Device and using the Device Selector window (for information, see [Using the Device Selector]);
- **Interface**—Drop-down menu listing for all interfaces on the selected device.

The Following VLANs Are Configured—A read-only panel that shows the VLANs, if any, that are configured on the currently selected Interface setting.

Port configuration and VLAN settings cannot be performed when editing objects— you are limited to selecting a different port (from the same device or from a different device) to be bound to the current object.

### Defining Port Reservations for an Infoblox Grid Member

**Note:** Editing Grid members does not allow for port configuration when you create or change a port reservation. For Grid member editing, you can select interfaces but you cannot edit them, such as setting the Admin Status to Up or choosing the Data VLAN or Voice VLAN. This section applies only to creating and defining port reservations and configurations for new Grid members. For the complete Grid member creation procedure, see [Adding Grid Members](#).

You can configure port reservations for a Grid member, including HA members, in the Add Grid Member wizard. All interfaces on a member (LAN1, LAN2, HA and MGMT) may have independently defined port reservations. For Grid members, port reservations are not subject to scheduling and workflow approval, and Grid Manager executes them immediately.

### Defining Port Reservations for an HA Pair

The process of defining port reservations and port configurations for a Grid member allows these settings to be defined during the creation of the new member. You can also edit them afterwards. Before performing this procedure, consult the sections [Planning for an HA Pair](#), [About HA Failover](#) and [Adding an HA Member](#) for more details.

1. Go to Grid -> Grid Manager and choose Add -> Grid Member from the vertical toolbar. Define your new HA Pair's settings and click Next.
2. In the second Add Grid Member Wizard step (Step 2 of 5), click the High Availability Pair option and enter the required Virtual Router ID value.
3. As with a normal HA pair configuration, enter the IP information about the following interfaces: VIP, Node 1 HA and LAN1 ports, Node 2 HA and LAN1 ports. The VIP address and the IP addresses for all the ports must be in the same subnet. Follow the guidelines provided in the section [Adding an HA Member](#).
4. Ensure all settings are correct and click Next.
5. The following step in the Add Grid Member Wizard presents a workflow that must be performed three times for each appliance—once for each of the three interfaces (LAN1, HA and MGMT) participating in the HA pair. (LAN2 may be configured by editing the Grid member afterwards.)

![Figure 15.20 Beginning the HA Pair Configuration's Port Reservations](#)
a. Select the Reserve Port check box. The Node1 -> LAN1 port listing changes to read Pending.
b. Click Select Device to choose the device (switch or switch-router) that is Node 1 of the HA Pair. (For information, see Using the Device Selector.)
c. After selecting the device, click OK.
d. Choose the device port for Node 1’s LAN1 port by choosing it from the Interface menu. The panel The Following VLANs are configured refreshes to show any VLANs that are currently provisioned on the selected port.
  e. (This step is optional.) Select the Configure Port check box.
  f. (This step is optional.) If the Data VLAN setting is enabled, select the VLAN from the Data VLAN menu.
  g. (This step is optional.) Choose an Admin Status of Up.
  h. (This step is optional.) Enter a Description.
  i. For the Node 1 -> HA port, follow steps 6a through 6h for that appliance port. Ensure you select the same switch and Data VLAN settings.
  j. For the Node 1 -> MGMT port, follow steps 6a through 6h for that appliance port. Ensure you select the same switch and Data VLAN settings.

8. Click Next when finished with the Reserve Port and optional Configure Port settings for all interfaces. The result appears similar to the example shown in Figure 15.21.

Figure 15.21 Port Reservations for an HA Pair
Editing Port Reservation Settings for an Infoblox Grid Member

Editing an existing Grid member's port reservation does not permit configuring the currently selected port. You can select ports from any device to change the port reservation. For any selected device, ports with an Operational Status of Down appear in the Interface list. For editing Grid member settings, you can select interfaces but you cannot configure them; setting the Admin Status to Up or choosing the Data VLAN and changing the Description are not allowed when editing a Grid member.

Figure 15.23 Editing a Grid Member's Port Reservation Settings
You can edit any appliance’s port reservation settings:

1. Go to Grid -> Grid Manager and select the check box for the Grid member you wish to edit. Click Edit from the vertical toolbar.
2. Click the Port Reservation tab.
3. Select the Reserve Port check box. The Node1 -> LAN1 port listing changes to read Pending.
4. Click Select Device to choose the device. (For information, see Using the Device Selector.)
5. After selecting the device, click OK.
6. Choose the device interface from the Interface menu. Click Save & Close when finished.

On HA pairs the process is quite similar except that you may edit up to the full complement of interfaces used for each appliance in the HA pair. The Grid Member Properties Editor supports all ports for each appliance in the HA Pair.

**Note:** When editing Grid members and HA Grid members, Grid Manager does not allow changes to VLAN settings, Admin Status or port description in the editor. You can change these values in the Interfaces table by double-clicking the table row for the interface you want to edit.

### Defining Device Information

During the process of configuring a port reservation for an IPAM object, you can define device information settings as descriptive information for IPAM objects, as seen in Figure 15.24.

**Figure 15.24 Device Information Settings for IPAM Objects in the Wizard**
If you define Device Information and Device Vendor settings for a port reservation, which are optional, and choose to discover the object to which the port reservation is associated, you may see a conflict if discovery of the object finds that the device for the port reservation is a different type or different vendor. For example, if the specified information states that the device is a switch, and the discovered device is a router, Network Insight reports a conflict. Another example: you declare the vendor to be Aruba, and the discovered value is Cisco. For information on resolving such conflicts, see Resolving Port Reservation Conflicts.

The Device Type menu provides the following settings:

- ESX Server—identifies the object as a VMware ESX host.
- MSFT Server—identifies the object as a Microsoft Hyper-V host.
- Net MRI—NetMRI appliance from Infoblox;
- NIOS—Infoblox appliance;
- Router—Provides routed connections, including VLANs;
- Switch—provides L2 switched connections only;
- Switch-Router—Provides L2/L3 switched connectivity, including VLANs;
- VNIOS—Infoblox virtual appliance.

The Device Vendor menu provides the following device vendor choices:

- Cisco
- Juniper
- Infoblox
- Aruba
- Dell
- HP

IPAM object wizards allow definition of the settings when you create the object, or you can define the settings later.

### Defining Blackout Periods

**Note:** You can separately define blackout periods for discovery, and for port configuration. This section describes how to use the blackout feature for discovery. For more information on blackouts for port configuration tasks, consult the section Defining Port Configuration Blackout Periods.

Discovery protocols can occupy significant resources within the network when discovery is taking place. While you can schedule any discovery or port control task for any single time period or recurring time period, you can also establish time periods when Network Insight does not talk to devices or networks for discovery.

You can define blackout settings at two levels in Grid Manager:

- Under Grid Discovery Properties, applying across the entire Grid;
- All networks managed by the Grid inherit discovery blackout settings by default;
- For individual networks under IPAM and under DHCP.
  - A network must be Managed before you can edit its discovery blackout settings.
  - Under IPAM, you can define discovery blackout settings for Network Containers and for networks (for DHCP, you can also set blackouts for DHCP Ranges);
  - If a network is in Managed state, it can be edited under IPAM or under DHCP for discovery settings and discovery blackout settings.

Discovery tasks may already be running when a blackout period takes effect. Current tasks are not interrupted and will complete within their time. Network Insight does not activate new discovery tasks during the blackout period, however.

### Defining Blackout Periods for the Grid

This procedure also covers defining port configuration blackout periods for the Grid. To define blackouts for the Grid:

1. From the Grid tab, select the Grid Manager tab, and click Edit -> Grid Discovery Properties. If you do not select an appliance from the list, the Grid Discovery Properties option remains enabled.
2. Expand the Toolbar and click Edit -> Grid Discovery Properties.
3. Click the Blackout tab.
4. Select the Enable Discovery Blackout check box and click the Scheduling icon to open a separate scheduling window. The Blackout Scheduler dialog opens.

   a. Select how often you want to execute the blackout period. You can select Once, Daily, Weekly, or Monthly.
   b. If you select Once, enter the day in the date picker and select a month from the drop-down list.
      - Enter a time in the hh:mm:ss AM/PM format. You can also select a time from the drop-down list.
      - Choose the Time Zone.
      - Specify the Duration: 1 or more Minutes, Hours or Days.
   c. If you select Daily, click either Every Day or Every Week day.
      - Enter a time in the hh:mm:ss AM/PM format. You can also select a time from the drop-down list.
      - Choose the Time Zone.
      - Specify the Duration: 1 or more Minutes, Hours or Days.
   d. If you select Weekly, complete the following:
When a scheduled Grid-level blackout period goes into effect, no operations related to discovery take place for the specified time period across the Infoblox Grid. Any discovery tasks already in progress will run to completion but no new ones will start.

Defining Blackout Periods for Networks

Network Insight offers considerable flexibility in how you apply blackout periods. You may choose to have discovery allowed for most managed networks but elect to have a discovery blackout for selected networks that are traffic- or latency-sensitive. You can define extended time periods and regularly scheduled times when discovery and/or port configuration tasks is not in progress on a specific IPAM network or within a network container. By default, the network inherits its discovery blackout settings from the Grid level. Editing a network under IPAM or DHCP, blackout settings apply only to the specified network. You also specify the scheduled time when the blackout period begins, and the duration of the blackout period.

As noted, a network must be in managed status before editing discovery or blackout features. To define a discovery blackout for a network under IPAM or DHCP:

1. Select a managed network from one of the following locations:
   a. Data Management → IPAM → list view
      --or--
   b. Data Management → DHCP → Networks
2. Click the Action icon
   next to the network you want (this automatically selects it) and select Edit from the menu. The Edit Network dialog appears.
3. Click the Discovery Blackout tab.
4. Click Override to change blackout settings for the chosen network.
5. Select the Enable Discovery Blackout check box and click the Scheduling icon to open a separate scheduling window. (Because the settings are inherited, Enable Discovery Blackout may or may not already be enabled.) The Blackout Scheduler dialog opens.
   a. Select how often you want to execute the blackout period. You can select Once, Daily, Weekly, or Monthly.
   b. If you select Once, enter the day in the date picker and select a month from the drop-down list.
      • Enter a time in the hh:mm:ss AM/PM format. You can also select a time from the drop-down list.
      • Choose the Time Zone.
      • Specify the Duration: 1 or more Minutes, Hours or Days.
   c. If you select Daily, click either Every Day or Every Weekday.
      • Enter a time in the hh:mm:ss AM/PM format. You can also select a time from the drop-down list.
      • Choose the Time Zone.
      • Specify the Duration: 1 or more Minutes, Hours or Days.
   d. If you select Weekly, complete the following:
      • Under Schedule every week on:, select the check box for any day of the week.
      • Enter a time in the hh:mm:ss AM/PM format. You can choose a time from the drop-down list.
      • Choose the Time Zone.
      • Specify the Duration: 1 or more Minutes, Hours or Days.
   e. If you select Monthly, complete the following:
      • Schedule the day of the month: A discovery blackout can be executed monthly on a specific day, or instances can be executed more than one month apart on a specific day, in the Day every month(s) field.
      • Enter a time in the hh:mm:ss AM/PM format. You can choose a time from the drop-down list.
      • Choose the Time Zone.
      • Specify the Duration: 1 or more Minutes, Hours or Days.
6. If necessary, select the Enable Port Configuration Blackout check box and click the Scheduling icon to open the scheduling window.
   For information, see Defining Port Configuration Blackout Periods.
7. Follow Steps 5a–5e to schedule the port configuration blackout for the chosen network. (For related information, see Defining Port Configuration Blackout Periods)
   --or--
   Select the Use Discovery Blackout Schedule check box to apply the discovery blackout schedule defined for the network.
8. When you have finished configuring schedules for blackout periods for the network, click Save & Close.

When a scheduled blackout goes into effect, no operations related to discovery and/or port configuration take place for the specified time period on the selected network. Any related operations in progress will run to completion but no new ones will start.
Defining Port Configuration Blackout Periods

Similar to discovery blackout periods, you can define port configuration blackout periods for managed networks under IPAM and DHCP. You specify the scheduled time when the blackout period begins, and the duration of the blackout period. By default, networks inherit their blackout settings from the Grid level. For port configuration blackout settings in a network, the network must be under managed status in IPAM.

Defining Port Configuration Blackouts for the Grid

Port configuration blackout settings apply globally across the entire Infoblox Grid unless overridden by members or for specific networks.

1. From the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and click Edit → Grid Discovery Properties.
3. Click the Blackout tab.
4. Click the Enable Port Configuration Blackout check box.
   a. Select the Use Discovery Blackout Schedule check box to apply the same blackout schedule to port configurations that is applied locally to discovery blackouts. (For more information on discovery blackouts, see Defining Blackout Periods 61.)
   b. Click the Schedule icon below. The Blackout Scheduler dialog opens.

Figure 15.25 Scheduling a Port Configuration Blackout

Defining Port Configuration Blackouts for Networks

By default, networks inherit their blackout settings from the Grid level. You can override these with local settings for the network or for a network container, for both IPAM and DHCP. To change port configuration blackout settings for an IPAM or DHCP network or network container:

1. Select a managed network or network container from one of the following locations:
   a. Data Management → IPAM → list view
      –or–
   b. Data Management → DHCP → Networks
2. Click the Action icon
   🌡️
   for a chosen network and choose Edit from the popup menu.
   - Under IPAM, the network must be in managed status (a value of Yes appears in the Managed field, and the table row is highlighted in white).
   - Under DHCP, all networks appearing on this page may be selected for this purpose.
3. Click the Discovery Blackout tab. The editor page appears as shown in Figure 15.26: The Discovery Blackout tab with enabled Port Configuration Blackouts
Conflict Resolution in Network Insight

Figure 15.27 Locating Conflicts and Beginning Their Resolution

You can sometimes encounter conflicts when defining port reservations for IPAM-managed objects such as Fixed IP addresses or host records. The quickest way to locate any conflicts in Grid Manager is to open the Conflicts Smart Folder as noted in Figure 15.27.

Numerous types of conflicts are possible:

- Device Information conflict;
- Port Reservation conflict, including Used Port Reservation conflicts (usually resulting from a request to reserve a port that has already been assigned to another IPAM object);
- Fixed address conflict;
- IP Address conflicts;
- DHCP Range conflicts (such as: Discovered address is within an existing DHCP range but does not match an existing lease, fixed address, or exclusion range);
- MAC Address conflict (such as: Discovered MAC Address conflicts with existing fixed address).

Note: When you execute discovery (Discovery -> Discovery Now from the Toolbar), the appliance does not send SNMP trap if it finds any conflicting information between the NIOS data and the discovered data.

The Conflict Resolution wizard automatically recognizes the object associated with the conflict (which is listed in the Related Objects pane as noted in Figure 15.27) and ensures that changes you make during resolution are applied correctly to the object. An example appears in Figure 15.
Resolving Port Reservation Conflicts

Sometimes, administrators may accidentally request a device port to be reserved for an IP address when the port is already reserved for another object, or try to apply a different port to an object that already has a port reservation. When these cases arise, Grid Manager reports a conflict. To resolve port reservation conflicts:

1. Click the link provided in the Conflicts Smart Folder.
2. Expand the Toolbar and click Resolve Conflict, as shown in Figure 15.27.
   
   The Resolve Port Reservation Conflict dialog opens, showing the differences between the reserved and discovered information.
3. Choose from the following options:
   - Change the reserved port to be the same as the discovered port.
   - Keep the configured port reservation and clear the conflict for the next 1 day(s).

   **Note:** In the Grid Discovery Properties → Advanced tab, the Ignore Conflict Duration setting governs the default time duration to ignore (clear) certain types of conflicts that may occur when defining IPAM objects that are associated with discovered and managed devices, interfaces, or IP addresses. Increments can be defined in Hours or Days. For more information, see Defining Seed Routers for Probe Members.
4. Click OK to save changes.

   **Note:** For other conflict examples, see Resolving Multiple Conflicts.

Another category of conflicts involves incorrectly defined device information for the object:

- The reserved Device Type information provided is different from the discovered vendor and device type (Router vs. Switch, for example);
- The defined Device Vendor information does not match with the discovered information.
- A User Port Reservation conflict occurs when an unmanaged IP address attempts to use a port that is already reserved by an IPAM object on a different IP address.

You can choose from the following options:

- Change configured information to discovered information.
- Keep the current device configuration and clear the conflict for the next 1 day(s).

In virtually all cases, replacing the configured information with the discovered information successfully clears the conflict; click OK to commit changes or to temporarily clear the conflict.

**Resolving Multiple Conflicts**

You can define objects for IP addresses, attempt to apply a port reservation, or incorrectly specify a value such as a MAC address or a vendor name, and accidentally cause multiple conflicts after creating the new object.

When multiple conflicts need to be resolved for a particular IP address, you use a Resolve Multiple Conflicts wizard:

1. To quickly locate any conflicts, open the Smart Folders panel and open the Conflicts list.
2. Click the IP address for any entry in the Conflicts list. The IPAM page opens for the selected IP address, with the top panel highlighted in pink to indicate the conflict.
3. Open the vertical toolbar and click Resolve Conflict.
4. If multiple issues are involved with the conflict entry, the Resolve Conflicts wizard lists each of them as shown in Figure 15.29.
a. In this case, the MAC address specified in the last fixed address object configuration, for that object, conflicts with the discovered MAC address associated with the IP. (You can verify this by checking the Related Objects tab in the IPAM page for the IP address.) Choose from one out of two options:

- **Change the configured MAC address to be the same as the discovered MAC address**;
- **Keep fixed address and ignore this conflict for the next 1 day(s)**.

In this example, the Discovered information for the MAC address associated with the Fixed Address object is one digit off from the Existing MAC information, which was entered incorrectly by the administrator. The Discovered MAC, shown in red, is the correct value and should be used to overwrite the record for the conflict.

a. To resolve the conflict, the Configured information must be overwritten with the Discovered information:
Part 4 DNS

This section describes how to configure the Grid to provide DNS services. It includes the following chapters:

- Chapter 16, Infoblox DNS Service,
- Chapter 17, Configuring DNS Services,
- Chapter 18, DNS Views,
- Chapter 19, Configuring DNS Zones,
- Chapter 20, DNS Resource Records,
- Chapter 21, Configuring DDNS Updates,
- Chapter 22, DNSSEC,
- Chapter 23 Managing DNS Traffic Control,
- Chapter 24, Configuring IP Routing Options,

Chapter 16 Infoblox DNS Service

The NIOS appliance uses a standard, BIND-based DNS protocol engine. It interoperates with any other name server that complies with the DNS RFCs (see DNS RFC Compliance).

This chapter provides an overview of the DNS configuration tasks. It includes the following sections:

- Configuring DNS Overview
  - DNS Configuration Checklist
- About Inheriting DNS Properties
  - Overriding DNS Properties
- Understanding DNS for IPv6
  - Configuring IPv6 on a Grid Member
  - Configuring DNS for IPv6 Addressing

Configuring DNS Overview

An overview of the DNS configuration process is outlined in the following diagram, illustrating the required steps for preparing a NIOS appliance for use:
DNS Configuration Checklist

The following checklist includes the major steps for configuring DNS:

Table 16.1 DNS Configuration Checklist

<table>
<thead>
<tr>
<th>Step</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decide if you want to configure DNS properties for the Grid and for individual members</td>
<td>Chapter 16, Infoblox DNS Service</td>
</tr>
<tr>
<td>Decide if you want to create a new DNS view, in addition to the default DNS view</td>
<td>Chapter 18, DNS Views</td>
</tr>
<tr>
<td>Decide which type of DNS zone you want to configure</td>
<td>Chapter 19, Configuring DNS Zones</td>
</tr>
<tr>
<td>Add hosts and resource records</td>
<td>Chapter 20, DNS Resource Records</td>
</tr>
<tr>
<td>Import zone data</td>
<td>Importing Zone Data</td>
</tr>
<tr>
<td>Enable DNS service on the member</td>
<td>Starting and Stopping the DNS Service</td>
</tr>
</tbody>
</table>

About Inheriting DNS Properties

You can configure DNS properties at the Grid, member, zone, and resource records level. The NIOS appliance applies the properties hierarchically, with the Grid at the top of the hierarchy. Grid settings apply to all members in the Grid, unless you override them at the member,
When you set DNS properties for a particular member, these properties override the Grid properties and apply to all zones served by that member. When you set properties for a specific zone, they override the member properties and apply to the resource records in the zone. You can also override the zone properties and set properties for specific resource records.

When you configure DNS properties that contain inherited values, the appliance displays the information based on the inheritance sources. There may be times when an object can inherit properties from different sources with different settings. The following table summarizes what the appliance can display:

<table>
<thead>
<tr>
<th>When you see...</th>
<th>it means...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherited From &lt;object&gt;</td>
<td>the DNS property has a definite value from an inheritance source.</td>
</tr>
<tr>
<td>Inherited From Upper Level</td>
<td>the appliance cannot yet determine the inherited value or inheritance source for the DNS property.</td>
</tr>
<tr>
<td>Inherited From Multiple</td>
<td>the DNS property has the same value that it inherits from multiple sources.</td>
</tr>
<tr>
<td>Settings Inherited from Multiple Ancestors, View Multiple Inheritance Scenarios</td>
<td>the DNS property has different values that it inherits from multiple sources, and you can view the values and their corresponding sources by clicking the View Multiple Inheritance Scenarios link.</td>
</tr>
</tbody>
</table>

Based on the information provided, you can then decide whether to override or keep the inherited values. You must have read/write permissions to the DNS resources to override inherited values. You can only view inherited values and paths if you have at least read-only permissions. In the example in Figure 16.1, the DNS zone is served by members with different query settings.

**Figure 16.1 DNS Zone with Different Inherited Settings**

The Multiple Inheritance Viewer indicates that the two servers have different query ACLs, as shown in Figure 16.2. You can then view the Query properties of each member and edit them, or override the setting and specify values that apply to the zone only.

**Figure 16.2 Multiple Inheritance Viewer**

**Overriding DNS Properties**

DNS properties configured at the Grid level apply to the entire Grid. You can choose to keep the inherited properties or override them when you configure the properties for a member, zone, or resource record.

To override an inherited value:

1. In a wizard or editor, click Override next to a property to enable the configuration. The Override button changes to Inherit.
2. Enter a new value to override the inherited value.
Understanding DNS for IPv6

You can configure NIOS appliances to provide DNS services over IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6) networks. You can configure the Grid member as IPv6, or dual-mode name server. Dual-mode name server is capable of sending and receiving IPv4 and IPv6 queries and responses. It can serve DNS data in response to both IPv4 and IPv6 queries. The appliance supports authoritative forward-mapping zones containing AAAA records mapping host names to IPv6 addresses, as well as authoritative reverse-mapping zones with PTR records mapping IPv6 addresses to host names. Configuring a Grid containing an IPv4 primary server and IPv6 secondary servers is not supported. You must enable IPv6 on both the primary and secondary servers within the Grid to enable them to communicate with each other.

Infoblox highly recommends that you enable IPv6 on your Grid appliances before configuring IPv6 authoritative zones. The NIOS appliance supports IPv6 configuration on multiple interfaces, such as LAN1, LAN2, MGMT, anycast (OSPF and BGP), and loopback interfaces. Infoblox integrates IPv6 address management into many of the same places where IPv4 addresses are entered. Data validation occurs on all IP address fields and automatic validation is done to ensure proper entry of either an IPv4 address or an IPv6 address. The NIOS appliance supports the following DNS functions for IPv6:

- AAAA records—You can import, serve queries, display, add, delete, and modify AAAA records on the appliance. An AAAA record is equivalent to an IPv4 A record, relying upon a forward-mapping zone to map a hostname to an IPv6 address. A single forward-mapping zone can map names to both IPv4 and IPv6 addresses. The appliance autogenerates AAAA records for any of its interfaces that have IPv6 addresses.
- Hosts—You can configure IPv4 and IPv6 addresses for hosts. For information, see Adding Host Records.
- ip6.arpa—A specific domain for IPv6 is used for DNS reverse lookups called ip6.arpa. This domain maps an IPv6 address to a hostname. When you specify an IPv6 network, the appliance automatically creates the appropriate zone under ip6.arpa.
- PTR records—Import, serve queries, display, add, delete, and modify PTR records within an ip6.arpa reverse zone. The PTR record returns a domain name corresponding to an IPv6 address contained in the ip6.arpa zone. The appliance does not autogenerate PTR records; the user must configure PTR records manually.
- DDNS—The appliance supports AAAA and PTR records for DDNS (Dynamic DNS).

For more information about DNS for IPv6, see RFC 3596, DNS Extensions to Support IP Version 6.

Address Structures

IPv4 uses a 32-bit, 4-octet (each octet separated by decimals) addressing structure to designate sources and destinations within a network. Since there are 32 bits that make up the address, IPv4 can support up to 4 billion unique addresses.

An IPv6 address is a 128-bit number in colon hexadecimal notation. It consists of eight groups of four hexadecimal digits separated by colons (example: 12ab:0000:0000:0123:4567:89ab:0000:cdef). Since there are 128 bits that make up the address, IPv6 can support up to $3.4 \times 10^{38}$ unique addresses. The increase in the number of unique IPv6 addresses is one of the biggest advantages of an IPv6 implementation.

Figure 16.3 IPv6 Address Structure

<table>
<thead>
<tr>
<th>n bits</th>
<th>m bits</th>
<th>128-n-m bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Routing Prefix</td>
<td>Subnet ID</td>
<td>Interface ID</td>
</tr>
</tbody>
</table>

The IPv6 address structure consists of the following:

- Global Routing Prefix—Global routing prefix is a (typically hierarchically-structured) value assigned to a site.
- Subnet ID—Subnet ID is an identifier of a link within the site.
- Interface ID—Interface Identifier. This portion of the address identifies the interface on the subnet. This is equivalent to the host identifier for IPv4 addresses.

When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab:0000:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered.

Configuring IPv6 on a Grid Member

You can configure a Grid member in either IPv6 or dual mode (IPv4 and IPv6) to support IPv6 connections. A dual mode Grid member supports both IPv4 and IPv6 connections by configuring an IPv6 address on the member, in addition to the standard IPv4 address. When you enable IPv6 on a member, you can manually enter the IPv6 gateway address or enable the member to automatically acquire the address from router advertisements. Routers periodically send router advertisements that contain link-layer addresses and configuration parameters. A NIOS appliance that supports IPv6 can listen for router advertisements and obtain the default gateway IP address and link MTU (maximum transmission unit). The link MTU is the maximum packet size, in octets, that can be conveyed in one transmission unit over a link. Thus you can set parameters on a router once and automatically propagate it to all attached hosts.

To configure the member to support IPv6:
1. From the Grid tab, select the Grid Manager tab -> Members tab.
2. Expand the Toolbar and click Add -> Add Grid Member.
3. In the Add Grid Member wizard, enter the following and click Next:
   - **Member Type**: Specify the appliance type of the Grid member. If the member is an Infoblox appliance, select Infoblox, which is the default. If the member is a NIOS virtual appliance, select Virtual NIOS.
   - **Host Name**: Type the FQDN (fully qualified domain name) of the appliance that you are adding to the Grid.
   - **Time Zone**: If the Grid member is in a different time zone from the Grid, click Override and select a time zone.
   - **Comment**: Type a comment that provides some useful information about the appliance, such as its location.
   - **Master Candidate**: Select this option to designate this appliance as a Master Candidate. For supported vNIOS appliances, see Supported vNIOS Appliance Models and Specifications. Note that the Grid Master Candidate must use the same communication protocol as the Grid Master.

4. Enter the following information about the member that you are adding to the Grid and click Next:
   - **Type of Network Connectivity**: Select IPv6 to configure an IPv6 Grid member or select IPv4 and IPv6 to configure a dual mode Grid member.
   - **Select Standalone Member** to configure a single member or select High Availability Pair to configure an HA member. For an HA member, enter the Virtual Router ID number and if the HA member is configured in dual mode, select IPv6 in the Send HA and Grid Communication Over field.
   - **Required Ports and Addresses**: This table lists the network interfaces based on the type of network connectivity of the Grid member. For IPv6 Grid member, specify the network information for LAN1(IPv6) interface. For a dual mode Grid member, specify the network information for both LAN1(IPv4) and LAN1(IPv6) interfaces. For IPv6 HA member, specify the network information for VIP (IPv6), Node1 LAN1(IPv6), and Node2 LAN1(IPv6) ports. For a dual mode HA member, specify the network information for the following interfaces: VIP (IPv4), Node1 LAN1(IPv4), Node2 LAN1(IPv4), VIP (IPv6), Node1 LAN1(IPv6), and Node2 LAN1(IPv6).

5. Save the configuration and click Restart if it appears at the top of the screen.

### Configuring DNS for IPv6 Addressing

Configuring the appliance to manage DNS services for IPv6 connections is similar to configuring DNS services for IPv4 connections. For simplicity, the IPv6 procedures are located in the same location as the corresponding procedures for IPv4 in this chapter. In most cases, the key difference within the procedure involves selecting an IPv6 mapping zone instead of an IPv4 mapping zone. You can configure the following tasks: Table 16.2 IPv6 DNS Configuration Checklist

<table>
<thead>
<tr>
<th>Step</th>
<th>For more information</th>
</tr>
</thead>
</table>
| Create primary or secondary name servers and specify an IPv6 root server. | • About Authoritative Zones  
• Specifying a Primary Server  
• Specifying Secondary Servers  
• Creating a Root Zone |
| Configure the IPv6 zones. | • Creating an Authoritative Forward-Mapping Zone  
• Creating an Authoritative Reverse-Mapping Zone |
| Configure IPv6 resource records | • Managing AAAA Records  
• Managing PTR Records |

Copyright ©2019, Infoblox, Inc. All right reserved.
Chapter 17 Configuring DNS Services

This chapter provides general information about DNS service properties. The topics in this chapter include:

- Configuring DNS Service Properties
- Configuring DNS Access Control
- About Time To Live Settings
- Configuring Hostname and Server ID Options
- Enabling and Disabling DNS Health Check Monitor
- Adding an Email Address to the SOA Record
- Notifying External Secondary Servers
- Enabling the Configuration of RRset Orders
- Specifying Port Settings for DNS
- Deleting PTR Records associated with A or AAAA Records
- Specifying Minimal Responses
- Starting and Stopping the DNS Service
- About DNS Cache
  - Clearing DNS Cache
  - Clearing Cache for DNS Views
  - Clearing Domains and Subdomains from DNS Cache
  - Viewing DNS Configuration
  - Viewing DNS Cache Details
  - Viewing Statistics
- Using Forwarders
  - Specifying Forwarders
- Controlling DNS Queries
  - Specifying Queries
- Enabling Recursive Queries
  - Enabling Recursion
  - Configuring Resolver Queries Timeout
  - Restricting Recursive Client Queries
  - Enabling Recursive Resolution Using EDNS Client Subnet (ECS)
  - Enabling DNS Fault Tolerant Caching
- Controlling AAAA Records for IPv4 Clients
  - Enabling AAAA Filtering
- About NXDOMAIN Redirection
  - About NXDOMAIN Rulesets
  - NXDOMAIN Redirection Guidelines
  - Configuring NXDOMAIN Redirection
  - Creating Rulesets
  - Enabling NXDOMAIN Redirection
- Detecting and Mitigating DNS DDoS Attacks
  - Automated Mitigation of Phantom Domain Attacks
    - Guidelines for Mitigating Phantom Domain Attacks
    - Configuring Parameters for Mitigating Phantom Domain Attacks
  - Detecting NXDOMAIN Attacks
    - Tracking NXDOMAIN Responses
    - Tracking Cache Hit Ratio of Recursive Queries
    - Tracking Dropped UDP Packets
- Mitigating Possible NXDOMAIN Attacks
- Support for RRL (Response Rate Limiting)
- About Blacklists
  - About Blacklist Rulesets
  - Blacklist Guidelines
  - Configuring the Blacklist Feature
  - Enabling Blacklisting
- Enabling Zone Transfers
  - Configuring Zone Transfers
  - Configuring Concurrent Zone Transfers
- About Root Name Servers
  - Specifying Root Name Servers
- About Sort Lists
  - Defining a Sort List
- Configuring a DNS Blackhole List
  - Defining a DNS Blackhole List
- Specifying Hostname Policies
  - Defining Grid Hostname Policies
  - Defining Hostname Restrictions
  - Obtaining a List of Invalid Record Names
- About DNS64
  - Configuring DNS64
Configuring DNS Service Properties
You can configure general DNS service properties and change some default values. The DNS service is disabled by default. To enable the member to provide DNS service, you must start the DNS service. For information about how to start and stop the DNS service, see Starting and Stopping the DNS Service. The following sections describe the DNS service properties that you can configure:

- Configuring DNS Access Control
- About Time To Live Settings
- Configuring Hostname and Server ID Options
- Adding an Email Address to the SOA Record
- Notifying External Secondary Servers
- Specifying Port Settings for DNS
- Specifying Minimal Responses
- Starting and Stopping the DNS Service

Configuring DNS Access Control
You can add ACEs (access control entries) or use a named ACL (access control list) to determine which hosts can perform specific DNS tasks. For information about how to define a named ACL, see Defining Named ACLs. When you add ACEs or a named ACL to Grid DNS properties, the configuration overrides member and object access control for DNS zone transfers, dynamic DNS updates, DNS queries and recursive queries, blackhole lists, and AAAA filtering. For a full list of operations that support access control, see Operations that Support Access Control.

To configure DNS access control:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. In the Grid DNS Properties editor, click Toggle Advanced Mode, and select one of the following tabs for specific DNS tasks:
   - Updates tab: Define ACEs or a named ACL to control Grid level dynamic DNS updates, as described in Enabling DNS Servers to Accept DDNS Updates.
   - Queries tab: Define ACEs or a named ACL to control Grid level DNS queries, recursive queries, and AAAA filtering, as described in Controlling DNS Queries, Enabling Recursive Queries, and Controlling AAAA Records for IPv4 Clients.
   - Zone Transfers tab: Define ACEs or a named ACL to control Grid level DNS zone transfers, as described in Enabling Zone Transfers. This does not apply to zone transfers for Microsoft servers. For information about Microsoft servers, see Setting Zone Properties.
   - Blackhole tab: Configure ACEs or a named ACL to define IP addresses and networks that you do not want to include during the DNS resolution process, as described in Configuring a DNS Blackhole List.
   - DNS64 tab: Configure ACEs or a named ACL for clients to which the appliance sends synthesized AAAA records DNS64 groups, as described in Setting DNS64 Group Properties.
3. Save the configuration.

You can override the Grid settings at the member and object levels.

About Time To Live Settings
You can specify TTL (time to live) settings for Infoblox host records and resource records. TTL is the time that a name server is allowed to cache data. After the TTL expires, the name server is required to update the data. Setting a high TTL reduces network traffic, but also renders your cached data less current. Conversely, setting a low TTL renders more current cached data, but also increases the traffic on your network.

You can specify global TTL settings at the Grid level, for individual zones, or resource records. When you configure TTL settings for auto-generated records, the following conditions apply:

- NS records that are auto-generated for delegated name servers use TTL settings from their delegated zones.
- Auto-generated glue A and AAAA records use TTL settings from a delegated zone if the name server is below the delegation point and does not belong to an authoritative child zone.
- All other auto-generated NS, A, and AAAA records continue to use TTL settings from their parent zones.
- Auto-generated PTR records do not inherit TTL settings from delegated zones. They use TTL settings from their parent zones.

When you have an RRSET (resource record set) that contains different TTL settings for each record, Grid Manager displays the actual TTL values for these records. However, in DNS responses, the appliance takes the least of the values and returns that as the TTL setting for all resource records in the RRset.

For recursive DNS servers, you can specify the maximum cache TTL value that establishes the time limit for the name server to cache positive responses. You can also specify the maximum negative cache TTL value that specifies the time limit for the name server to cache negative responses. For information about how to configure these settings, see Specifying Max Cache TTL and Max Negative Cache TTL Settings.
Specifying TTL Settings for a Grid

To specify global TTL settings for resource records hosted by Grid members:

1. From the Data Management tab, select the DNS tab and click the General tab -> Grid DNS Properties. In the Grid DNS Properties editor, select the Advanced tab (or click Toggle Advanced Mode). Member: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon. In the Member DNS Properties editor, select the General tab -> click the Advanced tab (or click Toggle Advanced Mode).
2. The TTL tab of the resource record editor displays the TTL setting the resource record inherited from the Grid or zone. Click Override and enter a value. The setting is in hours by default. You can change it to seconds, minutes, days or weeks.
3. Save the configuration and click Restart if it appears at the top of the screen.

Specifying TTL Settings for a Zone

To specify TTL settings for host and resource records in a zone:

1. From the Data Management tab, select the DNS tab and click the Zones tab -> dns view -> zone check box -> Edit icon.
2. In the Authoritative Zone editor, click Settings.
3. Click Override and complete the fields as described in the preceding section, Specifying TTL Settings for a Grid.

Specifying the TTL of a Host or Resource Record

To specify the TTL setting for an Infoblox host or resource record:

1. From the Data Management tab, select the DNS tab and click the Zones tab -> dns view -> zone -> resource_record.
2. The TTL tab of the resource record editor displays the TTL setting the resource record inherited from the Grid or zone. Click Override and enter a value. The setting is in hours by default. You can change it to seconds, minutes, days or weeks.
3. Save the configuration and click Restart if it appears at the top of the screen.

Specifying TTL Settings for a Lame Server

Servers that are marked as authoritative, but do not respond as authoritative servers are called lame servers. You can specify the number of seconds to cache a lame delegation or lame server indication through the Lame TTL option. Lame TTL usually indicates the amount of time your name server remembers information about the remote name server that is not authoritative for a zone, which is delegated to it. A domain or sub-domain that is delegated to a server that is not authoritative for the domain is called lame delegation. It indicates that a zone file does not exist for the domain on the server.

The lame time-to-live cache value can be defined at the Grid DNS, Member DNS, or DNS view level. To specify the Lame TTL cache value for a lame delegation or lame server:

1. Grid: From the Grid tab -> Grid Manager tab, select the DNS tab, click the Services tab -> member check box, expand the Toolbar and click Edit -> Grid DNS Properties. In the Grid DNS Properties editor, select the General tab -> click the Advanced tab (or click Toggle Advanced Mode). Member: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon. In the Member DNS Properties editor, select the General tab -> click the Advanced tab (or click Toggle Advanced Mode).
2. In the Grid DNS Properties, Member DNS Properties, or the DNS View editor, select the General tab -> click the Advanced tab (or click Toggle Advanced Mode) and then complete the following: Lame TTL: Specify the duration of time to cache a lame delegation or lame server. The default value is 600 seconds (ten minutes) and the maximum value is 1800 seconds (thirty minutes). The appliance displays a warning message when you specify a value equal to 0 (zero). The value 0 (zero) disables lame caching and is not recommended. The appliance displays an error message when you specify a value greater than 1800 seconds. Lame TTL cache value is inherited from the Grid by the member and DNS view levels and this field is disabled, by default. To override the Lame TTL cache value, click Override. You can override the value at the member and DNS view levels. To retain the same Lame TTL value as the Grid, click Inherit at the member and DNS view level.
3. Save the configuration and click Restart if it appears at the top of the screen.

Specifying Max Cache TTL and Max Negative Cache TTL Settings

You can specify the maximum duration of time for which your name server caches positive responses using the Max Cache TTL settings. The Max Cache TTL indicates the time limit for which the name server retains records in the cache. When the Max Cache TTL for a record expires, the name server deletes the record from the cache.
You can also specify the maximum duration of time for which your name server caches negative responses through the Max Negative Cache TTL settings. The Max Negative Cache TTL sets the time limit for which the name server retains negative responses (NXDOMAIN/NXRRSET responses) in the cache. The name server deletes a negative response from the cache when the Max Negative Cache TTL period for the entry expires.

You can define the Max Cache TTL value and the Max Negative Cache TTL value at the Grid DNS, Member DNS, and DNS view levels. To specify the Max Cache TTL and the Max Negative Cache TTL:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the toolbar and click Grid DNS Properties. **Member:** From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
2. **DNS View:** From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view check box -> Edit icon.
3. In the Grid DNS Properties, Member DNS Properties, or the DNS View editor, click Toggle Advanced Mode if the editor is in the basic mode.
4. Click the Advanced subtab of the General tab and then complete the following:
   - **MaxCacheTTL:** Specify the maximum duration of time for which the name server caches positive responses. Select the time period in minutes, hours, or days from the drop-down list. The default value is one week (7 days), and the maximum value is 49710 days, 1193046 hours, or 71582788 minutes. The appliance displays an error message when you enter a value greater than the maximum value. Note that setting the Max Cache TTL value to 0 (zero) will disable the name server from caching any data, and it is not recommended.
   - **MaxNegativeCacheTTL:** Specify the maximum duration of time for which the name server caches negative responses. Select the time period in minutes, hours, or days from the drop-down list. The default value is three hours, and the maximum value is 7 days, 168 hours, or 10080 minutes. The appliance displays an error message when you enter a value greater than the maximum value. Note that setting the Max Negative Cache TTL value to 0 (zero) will disable the name server from caching negative responses, and it is not recommended.

   The Max Cache TTL value and the Max Negative Cache TTL value are inherited from the Grid at the member and DNS view levels. To override the inherited values, click Override and specify the new value. To retain the Grid values, click Inherit.

Configuring Hostname and Server ID Options

When you configure DNS anycast, multiple DNS name servers share a single IP address. To identify which DNS name server is answering queries, you can configure the hostname and server ID options so the appliance returns the hostname of the DNS name server that is currently answering queries. By default, the hostname and server ID options are disabled on the NIOS appliance. You can configure the hostname bind directive and server-id directive options at the Grid level and override them at the member level. The appliance returns the hostname of the DNS name server that is currently answering queries when a client queries for the hostname.bind or the id.server with record type as TXT and class CHAOS, as follows:

```
dig @<IP> hostname.bind txt CH
dig @<IP> id.server txt CH
```

To secure the identity of the internet-facing DNS servers, you can configure the hostname and server ID options for specific Grid members that are internet-facing to return a user defined value instead of the real hostname. Alternatively, you can disable the hostname and server ID options at the Grid level and configure them only for those members that are not internet-facing. To configure the hostname and server ID options:

1. **Grid:** From the Data Management tab, select the DNS tab, and then select Grid DNS Properties from the Toolbar. **Member:** From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
2. In the Grid DNS Properties or the Member DNS Properties editor, click Toggle Advanced Mode if the editor is in the basic mode.
3. Click the Advanced subtab of the General tab and then complete the following:
   - **Hostname bind directive:** Select either Hostname or None from the drop-down list. The default is None. If you select Hostname, the appliance returns the hostname of the DNS name server that is currently answering queries. Selecting None disables the Hostname bind directive option.
   - In the Member DNS Properties editor, you can also select User defined and specify any hostname of your choice. The appliance returns the specified hostname instead of the real hostname of the DNS name server that is currently answering queries.
   - To override an inherited setting from the Grid, click Override. To retain the same setting as the Grid, click Inherit.
   - **Server-id directive:** Select either Hostname or None from the drop-down list. The default is None. If you select Hostname, the appliance returns the hostname of the DNS name server that is currently answering queries, when a client queries to identify the server ID of the name server that is answering queries.
   - Selecting None disables the Server-id directive option.
   - In the Member DNS Properties editor, you can also select User defined and specify a value of your choice. The appliance returns the specified value when a client queries to identify the server ID of the DNS name server that is answering queries.
   - To override an inherited setting from the Grid, click Override. To retain the same setting as the Grid, click Inherit.

4. Save the configuration and click Restart if it appears at the top of the screen.

Enabling and Disabling DNS Health Check Monitor

You can enable the DNS health check monitor to monitor whether the DNS server is responding to client requests. When you enable this feature, the appliance sends a query to the DNS server and waits for the response until the specified timeout duration. If the appliance is unable to receive a response from the DNS server after the specified number of retries, the appliance sends SNMP traps and email notifications about the failure. The appliance performs the DNS health check periodically based on the specified time interval.

**WARNING:** The DNS Health Check monitor might not work properly if DNS blackhole feature is enabled or if any named ACL is blocking the quer
To enable or disable the DNS health check monitor:

1. Grid: From the Data Management tab, select the DNS tab, and then select Grid DNS Properties from the Toolbar.
2. Member: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
3. Click the Advanced subtab of the General tab and then complete the following:
   - Enable DNS Health Check: This check box is deselected by default, meaning the DNS health check monitor is disabled. Select this check box to enable the DNS health check monitor and specify the following:
     - Interval: Enter the time interval in seconds. The interval value is measured from the end of the previous monitoring cycle. The default is 30 seconds. You can enter a value between 10 and 21600 seconds.
     - Timeout: Enter the timeout value in seconds. This is the time the appliance waits for a response to the query. The default is 3 seconds. You can enter a value between 1 and 10 seconds.
     - Retries: Enter the number of times the appliance tries to send the query after a failed attempt. The default is 3. You can enter a value between 1 and 10.
4. Save the configuration.

Adding an Email Address to the SOA Record

If the primary name server of a zone is a Grid member, you can add an administrator email address to the SOA record to help admins determine who to contact about this zone.

Adding an Email Address for SOA Records in the Grid

If all zones hosted by the Grid members have the same administrator, you can add the email address once for the Grid. The appliance then adds the email address to the RNAME field of the SOA records of the zones.

To add an email address to the SOA records at the Grid level:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. In the General -> Basic tab of the Grid DNS Properties editor, enter the email address in the E-mail Address (for SOA RNAME field) field.

   **Note:** The appliance does not support IDN for the E-mail Address (for SOA RNAME field) field at the Grid level. You can add an email address containing IDN for the SOA records at the zone level.

3. Save the configuration and click Restart if it appears at the top of the screen.

Adding an Email Address for the Zone SOA Record

To add an email address to the SOA record of a zone:

1. From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view -> zone check box -> Edit icon.
2. In the Authoritative Zone editor, click Settings.
3. Click Override beside the Email address (for SOA RNAME field) field and enter the email address of the zone administrator.
4. Save the configuration and click Restart if it appears at the top of the screen.

   **Note:** The appliance supports IDN for the host name of the Email address (for SOA RNAME field) field. For example, you can create admin@. but not @..com.

Notifying External Secondary Servers

Grid members can use database replication to maintain up-to-date zone data sets, so the secondary servers in the Grid can keep their zone data synchronized even if the primary server fails. Any external secondary servers can fall out of sync, however, if they rely only on the primary server to send notify messages when there is new zone data. Therefore all authoritative name servers in a Grid (all primary and secondary servers) send notify messages to external secondary servers by default. This ensures that an external secondary name server receives notify messages when its master is a secondary name server in a Grid. However, it also increases the number of notify messages.

Infoblox recommends that you do not configure a large number of external secondary servers in stealth mode. To ensure that these secondary servers receive notifications about zone updates, you can allow zone transfers for these IP addresses and then enable the appliance to add them to the also-notify statement. For information about how to configure this feature, see Configuring Zone Transfers.

To specify whether secondary name servers in the Grid are to send notify messages to external secondary name servers:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. In the Grid DNS Properties editor, click Toggle Advanced Mode.
3. When the additional tabs appear, click the Advanced subtab of the General tab.
4. Complete the following:
   - Enable Grid secondaries to notify external secondaries: This option is enabled by default.
- Notify Delay: Specify the number of seconds that the Grid secondary servers delays sending notification messages to the external secondaries. The default is five seconds.

5. Save the configuration and click **Restart** if it appears at the top of the screen.

For the external secondary servers to accept notify messages from the secondary name servers in the Grid and then request zone transfers from them, you must configure the external secondary servers to use the Grid secondary servers as the source of the zone transfers. This ensures that the external secondary servers continue to receive notify messages, even if the primary server is unavailable.

### Enabling the Configuration of RRSet Orders

You can use the Infoblox GUI to configure the order that the appliance uses to return the A and AAAA records associated with an Infoblox host. This feature is useful when you want the appliance to return the A and AAAA records of a host in a specific order. For example, if you want the management address to appear first on a list of IP addresses associated with a network device, you can configure the order of the IP addresses so the management address is always returned first on the list when you look up the name of the device. For information about using the Infoblox API to configure RRset order (resource record order) of a host, refer to the Infoblox API Documentation.

To specify an RRset order of a host record, you must first enable the feature at the Grid level. When you enable this feature and there are multiple IP addresses associated with the host record, you can specify one of the following RRset orders through the **Host Record** wizard and editor:

- **Fixed**: The A and AAAA records of the host are returned in the order that you specify in the IPv4 and IPv6 address tables.
- **Random**: The A and AAAA records of the host are returned in a random order.
- **Cyclic**: The A and AAAA records are returned in a round robin pattern.

For information about specifying RRset order of a host record, see [Adding Host Records](#). Note that when you configure an order type for the IP addresses associated with a host record, the order type applies to both the A and AAAA records of the host. It does not apply to any non-host A or AAAA records that may have the same owner name as the host record. By default, the appliance returns resource records in a cyclic or round robin order. The return order of non-authoritative data retrieved from a recursion is not affected by the host RRset order, and that remains cyclic.

When you enable the RRset order for hosts at the Grid level, you may not be able to maintain the same DNS responses on a recursive server if it exists in the Grid. You can preserve the original cached DNS responses by configuring a fixed RRset order on the recursive server so it can return A and AAAA records associated with domain names in the original order they were received. For information about configuring the RRset order for the cached DNS responses, see [Preserving the RRset Order for Cached DNS Responses](#).

To enable the configuration of RRset order for a host record:

1. From the **Data Management** tab -> **DNS** tab, expand the Toolbar, and then click **Grid DNS Properties**.
2. In the **Grid DNS Properties** editor, click **Toggle Advanced Mode**.
3. When the additional tabs appear, click the **Advanced** subtab of the **General** tab.
4. Complete the following:
   - **Enable setting RRset order for hosts with multiple addresses**: Select this check box to enable the configuration of RRset order for a host record. After you enable this feature, you can configure the RRset order in the **Host Record** wizard or editor. For information, see [Adding Host Records](#).
   - **Preserve host RRset order for Grid secondaries that use DNS zone transfers**: This is enabled only when you have enabled the setting of RRset order for host records. When you select this check box, the RRset order that you configure for a host record applies to the resource records of the Grid secondaries that are in the DNS transfer mode.

5. Save the configuration and click **Restart** if it appears at the top of the screen.

### Preserving the RRset Order for Cached DNS Responses

By default, when a client queries a domain name, the DNS caching appliance returns the A and AAAA records of the domain name in the cyclic order. However, this default behavior can be overridden if you have enabled and configured (at the Grid level) fixed RRset order for hosts that have multiple addresses. When you override the default behavior and preserve the fixed RRset order for cached DNS responses, the DNS caching appliance returns A and AAAA records associated with domain names in the order they were received from an upstream server. You can preserve the RRset order for the cached DNS responses and specify the fixed RRset order for A, AAAA, or both A and AAAA records at the Grid level and override the member and DNS view levels. Note that configuring fixed RRset order for specific FQDNs might slightly affect the performance of the DNS caching appliance.

To preserve the fixed RRset order for cached DNS responses at the Grid, member, or DNS view level:

1. **Grid**: From the **Data Management** tab -> **DNS** tab, expand the Toolbar, and then click **Grid DNS Properties**.
   - **Member**: From the **Data Management** tab, select the **DNS** tab and click the **Members** tab -> **member check box** -> **Edit** icon.
   - **DNS View**: From the **Data Management** tab, select the **DNS** tab -> **Zones** tab -> **dns_view check box** -> **Edit** icon.
2. In the editor, select the **RRset Order** tab -> click the **Basic** tab, and then complete the following:
   - **Enable fixed RRset order for following FQDNs**: Select this check box to preserve the configuration of RRset order for cached DNS responses.
   - In the **FQDN** table, specify the list of FQDN entries for which you want to preserve the RRset order. Note that you can configure a maximum of 25 FQDNs for the specified RRset order.
   - You can click the **Add** icon and complete the following to add a new entry to the list:
     - **FQDN**: Enter the fully qualified domain name with which the A or AAAA record is associated.

   **Note**: For Infoblox-4030, if you enter a wildcard character as part of the domain name, the appliance considers the wildcard character as a literal character. For example, if you enter test*.com, the appliance matches the domain name with test*.com only.

- **Record Type**: Select the record type from the drop-down list. You can select A, AAAA, or Both A and AAAA.
3. Save the configuration and click **Restart** if it appears at the top of the screen.
Specifying Port Settings for DNS

When requesting zone transfers from the primary server, some secondary DNS servers use the source port number (the primary server used to send the notify message) as the destination port number in the zone transfer request. If the primary server uses a random source port number when sending the notify message—that the secondary server then uses as the destination port number when requesting a zone transfer—zone transfers can fail if there is an intervening firewall blocking traffic to the destination port number.

Specifying a source port number for recursive queries ensures that a firewall allows the response. If you do not specify a source port number, the NIOS appliance sends these messages from a random port number. You can also specify a source for the DNS Traffic Control health check.

When performing recursive queries, the NIOS appliance uses a random source port number above 1024 by default. The queried server responds using the source port number in the query as the destination port number in its response. If there is an intervening firewall that does not perform stateful inspection and blocks incoming traffic to the destination port number, the recursive query fails.

You can specify a source port number for notify messages to ensure the firewall allows the zone transfer request from the secondary server to the primary server. If you do not specify a source port number, the NIOS appliance sends messages from a random port number above 1024.

You can limit if you have configured anycast and non-anycast IP addresses on the loopback interface, you must enable the appliance to provide DNS services on them. You can also configure the appliance to listen for DNS queries on a specific IP address that you configure on the loopback interface, by separating the source port for DNS queries from the port for notify messages and zone transfer requests. For information about the loopback interface and anycast addressing, see Using the Loopback Interface.

You can specify the source address settings for a Grid member and for DNS views assigned to a Grid member. Note that you can specify the source address settings for only specific DNS views that contain zones that are assigned to a Grid member. The static source port values for DNS views are inherited from the Member DNS properties.

Specifying Source Ports

To specify port numbers and settings for queries, notify messages and zone transfer requests for a Grid member or DNS view assigned to a Grid member:

1. **Member**: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
   - **DNS view**: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
2. In the editor, click Toggle Advanced Mode.
3. **Member**: When the additional tabs appear, click the Advanced subtab of the General tab.
   - **DNS View**: When the additional tabs appear, click the Advanced subtab of the DNS Views tab.
4. You can change the port settings as follows:
   - **Listen on these additional IP addresses**:
     - Click the Add icon to add an anycast or non-anycast address you configure on the loopback or VLAN interface. You must add all IP addresses you configure on the loopback or VLAN interface so the appliance can provide DNS services on them. Adding source ports for listening supports both IPv4 and IPv6 interfaces. For information about adding IP addresses on the loopback interface, see Using the Loopback Interface.
   - **Send queries from**:
     - If you want to improve the DNS service performance, you can separate the DNS queries from the notify messages and zone transfer requests. Select a value from the drop-down list to select an interface name: VIP, MGMT, LAN2, ANY, IP.
       - **IP Address**: This is displayed only when you select IP from the drop-down list. Specify the IP address of the source.
   - **Send notify messages and zone transfer requests from**:
     - From the drop-down list, select the source port of the notify messages and zone transfer requests that the Grid member sends. Select a value from the drop-down list to select an interface name: VIP, MGMT, LAN2, ANY, IP.
       - **IP Address**: This is displayed only when you select IP from the drop-down list. Specify the IP address of the source.

   **Note**: If you select IP addresses on the loopback or non-primary VLAN interface, then you must add these IP addresses in the Listen on these additional IP addresses table.

   - **Notify Delay**: Specify the number of seconds that the Grid secondary servers delays sending notification messages to the external secondaries. You can enter a value between 5 and 86400 seconds. The default is five seconds.
5. Save the configuration and click Restart if it appears at the top of the screen.

Specifying Static Source Ports

To specify static source ports for a Grid and Grid member:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   - **Member**: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
   - **DNS View**: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
2. In the editor, click Toggle Advanced Mode.
3. **Member**: When the additional tabs appear, click the Advanced subtab of the General tab.
   - **DNS View**: When the additional tabs appear, click the Advanced subtab of the DNS Views tab.
4. To override an inherited property, click Override next to it and complete the appropriate fields.
5. Complete the following:

   - **Set static source UDP port for queries (not recommended)**:
     - This is disabled by default. To override the value that has been inherited from the Grid, click Override. Select this check box to enable it and enter the UDP port number. You can enter a value between 1 and 65535. To retain the same value as the Grid, click Inherit.

   - **Set static source UDP port for notify messages**:
     - This is disabled by default. To override the value that has been inherited from the Grid, click Override. Select this check box to specify a source port for notify messages to ensure that the firewall allows the zone transfer request from the secondary server to the primary server. You can enter a value between 1 and 65399. If you do
not specify a source port, the appliance sends messages from a random port with a number above 1024. To retain the same value as the Grid, click Inherit.

5. Save the configuration and click **Restart** if it appears at the top of the screen.

### Using Extension Mechanisms for DNS (EDNS0)

The NIOS appliance supports EDNS0 (Extension Mechanisms for DNS), which allows DNS clients to expand and advertise up to 4096 bytes of UDP packets for certain DNS parameters. EDNS0 facilitates the transfer of UDP packets beyond the original restricted packet size of 512 bytes. As defined in RFC 6891, EDNS0 provides extended UDP packet size that supports additional DNS functionality, such as DNSSEC. When EDNS0 is supported, the DNS client adds information to the additional data section of a DNS request in the form of an OPT pseudo-RR (resource record). An OPT RR does not contain actual DNS data and its contents pertain to the UDP transport layer message only. An OPT RR is not cached, forwarded, or stored. For more information about EDNS0, refer to RFC 6891 *Extension Mechanisms for DNS (EDNS0)*.

EDNS0 is enabled on the NIOS appliance by default, which means all outgoing recursive queries are set to have a maximum UDP packet size of 4096 bytes. Typically, when the appliance receives a DNS request that contains an OPT RR, it assumes the DNS client supports EDNS0 and thus scales its response accordingly. When the appliance is used as a forwarder or a resolver for recursive queries and communicates with a client that does not support EDNS0, the appliance sends three queries starting with one that contains EDNS0 and DNSSEC support messages and is set to a maximum UDP packet size of 4096 bytes. When the first query fails, the appliance sends another query that contains only the EDNS0 support message. If the second attempt fails too, the appliance sends a third query that indicates a standard 512-byte query. Note that when EDNS0 is not used, DNS packets may be sent over TCP. For DNS service to function properly at this stage, ensure that you configure your firewall accordingly.

The following information demonstrates how the appliance responds when EDNS0 is enabled by default and the end server does not support EDNS0:

```
Packet 0954: 08:19:38.925 - query for www.google.com from Infoblox to forwarder (with EDNS0 support by setting the Extended Label Type to '01' and DNSSEC OK bit to '1')
Packet 139: 08:19:47.927 - query for www.google.com from Infoblox to forwarder (with EDNS0 support by setting the Extended Label Type to '01' and DNSSEC OK bit to '0')
Packet 1504: 08:19:58.929 - query for www.google.com from Infoblox to forwarder (without EDNS0 and DNSSEC support by sending a standard 512-byte query)
Packet 1505: 08:19:30:960 - query response for www.google.com from forwarder to Infoblox
```

To ensure that end servers that do not support EDNS0 can respond to recursive queries from the NIOS appliance and to improve DNS performance, you can disable EDNS0 for the Grid and override the Grid settings for individual members. Note that you cannot configure the maximum UDP packet size, which is set for 4096 bytes by default. When you disable EDNS0, the appliance does not include OPT RRs for all outgoing recursive DNS queries. Thus remote end servers that do not support EDNS0 can still respond to the queries. This feature is useful when your NIOS appliance is used as a forwarder or a resolver for recursive queries, and the end servers in the configuration do not support EDNS0.

To disable EDNS0:

1. **Grid**: From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Grid DNS Properties**. **Member**: From the **Data Management** tab, select the **DNS** tab and click the **Members** tab -> **member** check box -> **Edit** icon.
2. In the **Grid DNS Properties** or **Member DNS Properties** editor, click the **General** tab -> **Advanced** tab, and complete the following:
   - **Disable EDNS0**: This check box is deselected and EDNS0 is enabled by default. To override the value inherited from the Grid, click **Override**. To retain the same value as the Grid, click **Inherit**. Select this check box to disable EDNS0. When you disable EDNS0, the appliance does not include OPT RRs for all outgoing recursive DNS queries and all outgoing DNSSEC queries to zones within trusted anchors will fail even if DNSSEC validation is enabled.
3. Save the configuration and click **Restart** if it appears at the top of the screen.

### Deleting PTR Records associated with A or AAAA Records

You can configure the appliance to confirm whether to delete a PTR record when its corresponding A or AAAA record is being deleted. This feature is valid only if you have configured the appliance to automatically generate a PTR record when you create an A or AAAA record. For information about adding an A or AAAA record, see **Adding A Records** and **Adding AAAA Records**. When you delete a resource record, the appliance moves it to the Recycle Bin, if enabled. You can later restore it if needed. Note that this option is disabled by default for all new installations.

To enable this option:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Grid DNS Properties**.
2. In the **Grid DNS Properties**, click the **General** tab -> **Advanced** tab, and complete the following:
   - **Enable PTR record removal for A/AAAA records**: This check box is deselected by default. When you select this check box, the appliance displays the **Delete Confirmation** dialog box to confirm that you want to delete a PTR record associated with the A or AAAA record that is being deleted. For information about deleting an A or AAAA record, see **Modifying, Disabling, and Deleting Host and Resource Records**.
3. Save the configuration and click **Restart** if it appears at the top of the screen.

### Specifying Minimal Responses

A NIOS appliance returns a minimal amount of data in response to a query, by default. It includes records in the authority and additional data.
sections of its response only when required, such as in negative responses. This feature speeds up the DNS services provided by the appliance.

To disable returning minimal responses:

1. From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
2. In the Member DNS Configuration editor, click General -> Basic tab.
3. Clear the Return minimal responses check box.
4. Save the configuration and click Restart if it appears at the top of the screen.

Starting and Stopping the DNS Service

The DNS service is disabled by default. After you complete the DNS configuration, you can start DNS service on a member. You can also disable the DNS service on any Grid member. Be aware that disabling the DNS service on a member removes the NS records from it. If you later re-enable DNS service for this member, the NS records are then restored.

To start DNS service on a member:

1. From the Data Management tab, select the DNS tab -> Members tab -> member check box -> click the Edit icon.
2. In the Member DNS Properties editor, click General -> Basic tab, and do the following:
   - LAN1: Select IPv4 to start the DNS service using IPv4 or select IPv6 to start the DNS service using IPv6. Note that for a dual mode member, IPv4 will be selected by default.
3. Save the configuration.
4. Expand the Toolbar and click Start.
5. In the Start Member DNS Service dialog box, click Yes.
   Grid Manager starts the DNS service on the selected member.

You can stop DNS service on a member by selecting the member check box and click Stop from the Toolbar.

About DNS Cache

The NIOS appliance allows you to clear certain information from the DNS cache. You can do the following:

- Clearing DNS Cache
- Clearing Cache for DNS Views
- Clearing Domains and Subdomains from DNS Cache

Clearing DNS Cache

You can clear all the entries that are saved in the DNS cache. When you clear DNS cache on the NIOS appliance, entire BIND recursive cache is cleared.

To clear DNS cache:

1. From the Data Management tab, select the DNS tab -> Members tab -> member check box.
2. Expand the Toolbar, click Clear -> Clear DNS Cache.
3. Click Yes in the confirmation dialog box to clear DNS cache.

Clearing Cache for DNS Views

You can configure the NIOS appliance to clear cache of a specific DNS view. This feature clears cache entries of a specific DNS view that is associated with the selected member.

To clear cache of a DNS view:

1. From the Data Management tab, select the DNS tab -> click the Members tab.
2. Expand the Toolbar, click Clear -> Clear View's Cache.
3. Specify the following in the Clear View's Cache dialog box:
   - Member: Click Select Member to select a member. If there are multiple members, the Member Selector dialog box is displayed, from which you can select a member. Click the required member name in the dialog box. You can also click Clear to clear the displayed member and select a new one.
   - DNS View: Select a DNS View from the drop-down list. This list box appears only when there are multiple DNS views in the network view.
   - Click Clear Cache to clear the cache entries of the corresponding DNS View.

Note: The entire name server recursive cache is cleared, if you do not specify a DNS view when you clear cache using Clear View's Cache and Clear Domain Name features on the NIOS appliance.

Clearing Domains and Subdomains from DNS Cache

You can clear a specific domain and its subdomains from the DNS cache. When you clear a domain from the DNS cache, it is also removed from the BIND recursive cache.

To clear a specific domain and its subdomains:

1. From the Data Management tab, select the DNS tab -> click the Members tab.
2. Expand the Toolbar, click Clear -> Clear Domain Name.
3. Specify the following in the Clear Domain Name from Cache dialog box:
   - **Domain Name**: Enter a domain name you want to delete.
   - **Clear entire domain (including subdomains)**: Select the check box to clear the specified domain and its subdomains from the DNS cache. For example, if you enter corpxyz.com in the Domain Name field, then selecting this check box clears the entire domain including its subdomains such as www.corpxyz.com, corpxyz.com, x.corpxyz.com, etc. This check box is deselected by default.
   - **Member**: Click Select Member to select a member. If there are multiple members, the Member Selector dialog box is displayed, from which you can select a member. Click the required member name in the dialog box. You can also click Clear to clear the displayed member and select a new one.
   - **DNS View**: Select a DNS View from the drop-down list. This list box appears only when there are multiple DNS views in the network view.
   - Click Clear Domain Name to clear the domain name from the cache.

**Viewing DNS Cache Entries**

The NIOS appliance allows you to view certain information that is stored in the DNS cache. You can do the following:

- **Viewing DNS Configuration**
- **Viewing DNS Cache Details**
- **Viewing Statistics**

**Viewing DNS Configuration**

The NIOS appliance supports View Configuration feature that enables you to view DNS configuration details. You can view the configuration details through a browser.

To view DNS configuration:

1. From the Data Management tab, select the DNS tab -> click the Members tab.
2. Expand the Toolbar, click View -> View Configuration.

**Sample Output**

```plaintext
include "/infoblox/var/named_conf/tsig.key"

options {
    zone-statistics yes;
    directory "/infoblox/var/named_conf"; version none;
    hostname none; recursion yes;
    listen-on { 127.0.0.1; 10.34.1.18;);
    query-source address 10.34.1.18 port *; notify-source 10.34.1.18 port *; transfer-source 10.34.1.18;
    minimal-responses yes; max-cache-size 536870912; infoblox-top-query yes;
    infoblox-top-query-log-interval 60;
    infoblox-top-query-client 500;
    infoblox-top-query-name 500;
    infoblox-top-query-rr-type 500;
    infoblox-top-query-nxdomain 500;
    infoblox-top-query-servfail 500;
    infoblox-top-query-rpz 99;
    infoblox-top-query-rpz-items-per-client 100;
    lame-ttl 600;
}
for service restart: allow_bulkhost_ddns = Refusal allow-transfer { any; };
forwards { 10.32.0.177; };
avoid-v4-udp-portas ( 2114; 2113; 2115; 8000; 8089; 9997; 2222; 7911; 7912; 8000; 8089; 9997; 8080; 9000; 9999; 9004; 2022; 3374; 3115; 1194; };
transfer-format many-answers;
};

# Worker threads: default

# Bulk Host Name Templates:
#Four Octets: "$2-$3-$4" (Default)
#One Octet: "$4"
#Three Octets: "$2$3-$4"
#Two Octets: "$3-$4"
include "/infoblox/var/named_conf/dhcp_updater.key";
```
include "/infoblox/var/named_conf/rndc.key";

controls {
    inet 127.0.0.1 port 953
    allow { 127.0.0.1; } keys { "rndc-key"; };
};
logging {
    channel ib_syslog { syslog daemon; severity info; }
    category default { ib_syslog; }; category rpz { null; };
};

cache all_dns_views_updater_keys { key DHCP_UPDATER_default; key DHCP_UPDATER1; key DHCP_UPDATER3; };

---

**Viewing DNS Cache Details**

You can view data stored in cache for the DNS views that are configured in the NIOS appliance. You can view the details through a browser.

To view cache details:

1. From the **Data Management** tab, select the **DNS** tab -> click the **Members** tab.
2. Expand the Toolbar, click **View** -> **View Cache**.

**Sample Output**

```plaintext
;; Start view _default
;; Cache dump of view '_default' (cache _default)
;; $DATE 20121018180555
; authanswer a.test.com.23876IN A 4.4.4.4
;; Address database dump
;; Dump complete
```

---

**Viewing Statistics**

The **View Statistics** feature enables you to view DNS Statistics of a Grid member. You can view statistics through a browser.

To view statistics:

1. From the **Data Management** tab, select the **DNS** tab -> click the **Members** tab.
2. Expand the Toolbar, click **View** -> **View Cache**.

You can view statistics in the **DNS Statistics for Member** dialog box.

**Using Forwarders**

A forwarder is essentially a name server to which all other name servers first send queries that they cannot resolve locally. The forwarder then sends these queries to DNS servers that are external to the network, avoiding the need for the other name servers in your network to send queries off-site. A forwarder eventually builds up a cache of information, which it uses to resolve queries. This reduces Internet traffic over the network and decreases the response time to DNS clients. This is useful in organizations that need to minimize off-site traffic, such as a remote office with a slow connection to a company’s network.

You can select any Grid member to function as a forwarder. You must configure your firewall to allow that Grid member to communicate with external DNS servers. You can also configure the NIOS appliance to send queries to one or more forwarders.

You can define a list of forwarders for the entire Grid, for each Grid member, or for each DNS view.

**Specifying Forwarders**

To configure forwarders for a Grid, member, or DNS view:

1. **Grid**: From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Grid DNS Properties**.
2. **Member**: From the **Data Management** tab, select the **DNS** tab and click the **Members** tab -> **member check box** -> **Edit icon**.
3. **DNS View**: From the **Data Management** tab, select the **DNS** tab -> **Zones** tab -> **dns_view check box** -> **Edit icon**. Note that if there is only one DNS view—for example, the predefined default view—you can just click the **Edit icon** beside it.

To override an inherited property, click **Override next to it and complete the appropriate fields**.

2. Click the **Forwarders** tab.
3. Click the Add icon.
4. Enter an IP address in the text field. The field supports entry for both IPv4 and IPv6 values.
   - To remove a forwarder, select the IP address from the Forwarders list, and then click the Delete icon.
   - To move a forwarder up or down on the list, select it and click the Up or Down arrow.
5. To use only forwarders on your network (and not root servers), select the Use Forwarders Only check box.
6. Save the configuration and click Restart if it appears at the top of the screen.

Controlling DNS Queries

By default, the NIOS appliance responds to DNS queries from any IP address. You can create a list of queriers to which the appliance is allowed to respond; restricting it to specific networks, IP addresses, and remote servers that present specified TSIG (transaction signature) keys. When using TSIG keys, it is important that the appliances and servers involved with the authentication procedure use NTP (Network Time Protocol) for their time settings (see Using NTP for Time Settings).

In addition, you can also configure the appliance to respond to recursive queries. A recursive query requires the appliance to return requested DNS data, or locate the data through queries to other servers. Recursion is disabled by default. If you enable this feature, you can also create a list of allowed recursive queries. For information about allowing recursion, refer to Enabling Recursive Queries.

You can create a list of allowed queriers for the Grid and for individual Grid members.

Specifying Queries

To configure a list of allowed queriers for the Grid or for a member:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. Member: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.

To override an inherited property, click Override next to it and complete the appropriate fields.

1. In the Grid DNS Properties or Member DNS Properties editor, click Toggle Advanced Mode, select the Queries tab.
2. In the Allow queries from section, select one of the following:
   - Any: Select this if you do not want to configure access control for DNS queries. The appliance allows queries from all clients. This is selected by default.
   - Named ACL: Select this and click Select Named ACL to select a named ACL. Grid Manager displays the Named ACLs Select list. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this, the appliance allows clients that have the Allow permission to send and receive DNS queries. You can click Clear to remove the selected named ACL.
   - Set of ACEs: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list:
     - IPv4 Address and IPv6 Address: Select this to add an IPv4 address or IPv6 address. Click the Value field and enter the IP address of the remote querier. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.
     - IPv4 Network: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
       - Address: Enter an IPv4 network address and either a netmask or move the slider to the desired netmask.
       - Permission: Select Allow or Deny from the drop-down list.
     - IPv6 Network: In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
       - Address: Enter an IPv6 network address and select the netmask from the drop-down list.
       - Permission: Select Allow or Deny from the drop-down list.
     - TSIG Key: In the Add TSIG Key panel, complete the following, and then click Add to add the TSIG key to the list:
       - Key name: Enter a meaningful name for the key, such as a zone name or the name of the remote name server. This name must match the name of the same TSIG key on other name servers.
       - Key Algorithm: Select either HMAC-MD5 or HMAC-SHA256.
       - Key Data: To use an existing TSIG key, type or paste the key in the Key Data field. Alternatively, you can select the key algorithm, select the key length from the Generate Key Data drop-down list, and then click Generate Key Data to create a new key.
       - Any Address/Network: Select to allow or deny queries from any IP addresses.
         After you have added access control entries, you can do the following:
           - Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL icon, enter the name in the Convert to Named ACL dialog box. The appliance creates a new named ACL and adds it to the Named ACL panel. Note that the ACEs you configure for this operation stay intact.
           - Reorder the list of ACEs using the up and down arrows next to the table.
           - Select an ACE and click the Edit icon to modify the entry.
           - Select an ACE or multiple ACEs and click the Delete icon to delete the entries.
3. Save the configuration.

Enabling Recursive Queries

You can enable the appliance to respond to recursive queries and create a list of allowed networks, IP addresses, and remote servers that present specified TSIG (transaction signature) keys. When using TSIG keys, it is important that the appliances and servers involved with the authentication procedure use NTP (Network Time Protocol) for their time settings (see Using NTP for Time Settings).

A recursive query requires the appliance to return requested DNS data, or locate the data through queries to other servers. When a NIOS
appliance receives a query for DNS data it does not have and you have enabled recursive queries, it first sends a query to any specified forwarders. If a forwarder does not respond (and you have disabled the Use Forwarders Only option in the Forwarders tab of the Member DNS Properties editor), the appliance sends a non-recursive query to specified internal root servers. If no internal root servers are configured, the appliance sends a non-recursive query to the Internet root servers. For information on specifying root name servers, see About Root Name Servers.

You can enable recursion for a Grid, individual Grid members, and DNS views. For information about enabling recursion in a DNS view, see Configuring DNS Views. If you do not enable recursion, the appliance denies recursive queries from all clients.

Enabling Recursion

To enable recursion and create a list of recursive queriers:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. Member: From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon. To override an inherited property, click Override next to it and complete the appropriate fields.
2. In the Grid DNS Properties or Member DNS Properties editor, click Toggle Advanced Mode, select the Queries tab.
3. Click Allow recursion, and then in the Allow recursive queries from section, select one of the following:
   - None: Select this if you do not want to configure access control for recursive queries. When you select None, the appliance allows recursive queries from all clients. This is selected by default.
   - Named ACL: Select this and click Select Named ACL to select a named ACL. Grid Manager displays the Named ACLs Selectors. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this, the appliance allows clients that have the Allow permission to send and receive recursive DNS queries. You can click Clear to remove the selected named ACL.
   - Set of ACEs: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows.
     - IPv4 Address and IPv6 Address: Select this to add an IPv4 address or IPv6 address. Click the Value field and enter the IP address of the remote querier. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.
     - IPv4 Network: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
       - Address: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
       - Permission: Select Allow or Deny from the drop-down list.
     - IPv6 Network: In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
       - Address: Enter an IPv6 network address and select the netmask from the drop-down list.
       - Permission: Select Allow or Deny from the drop-down list.
     - TSIG Key: In the Add TSIG Key panel, complete the following, and then click Add to add the TSIG key to the list:
       - Key name: Enter a meaningful name for the key, such as a zone name or the name of the remote name server. This name must match the name of the same TSIG key on other name servers.
       - Key Algorithm: Select either HMAC-MDS or HMAC-SHA256.
       - Key Data: To use an existing TSIG key, type or paste the key in the Key Data field. Alternatively, you can select the key algorithm, select the key length from the Generate Key Data drop down list, and then click Generate Key Data to create a new key.
     - Any Address/Network: Select to allow or deny queries from any IP addresses. After you have added access control entries, you can do the following:
       - Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL button, and then in the Convert to Named ACL dialog box. The appliance creates a new named ACL and adds it to the Named ACL panel. Note that the ACEs you configure for this operation stay intact.
       - Reorder the list of ACEs using the up and down arrows next to the table.
       - Select an ACE and click the Edit icon to modify the entry.
       - Select an ACE and click the Delete icon to delete the entry. You can select multiple ACEs for deletion.
4. Save the configuration.

Configuring Resolver Queries Timeout

You can configure the amount of time that a recursive query will wait for a response before timing out. The default timeout behavior is to wait for 10 seconds before timing out.

To configure the resolver queries timeout value:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. Member: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon. To override an inherited property, click Override next to it and complete the appropriate fields.
2. In the Grid DNS Properties or Member DNS Properties editor, click Toggle Advanced Mode, select the Queries tab and complete the following:
   - Resolver queries timeout: Specify the maximum time allowed for a recursive query to wait for a response before timing out. You can enter either 0 or a value between 10 and 30 seconds. Setting the timeout value to 0 returns to the default timeout behavior, which is to wait for 30 seconds before timing out.
Restricting Recursive Client Queries

By default, the appliance can serve up to 1,000 outstanding recursive client queries. You can change this default value according to your business needs. After you configure the recursive client queries limit, you can enable the appliance to send SNMP traps for recursive queries. Enabling SNMP traps for recursive clients can help you identify possible flood attacks on the DNS recursive server. The appliance sends SNMP traps when the number of recursive client queries exceeds the configured thresholds. For information about how to set the threshold and reset values, see Defining Thresholds for Traps.

1. From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
2. In the Member DNS Properties editor, click Toggle Advanced Mode.
3. When the additional tabs appear, click the Advanced subtab of the Queries tab.
4. Select the Limit number of recursive clients to option and enter a number.
5. Save the configuration and click Restart if it appears at the top of the screen.

Enabling Recursive Resolution Using EDNS Client Subnet (ECS) Option

The EDNS Client Subnet (ECS) option is a DNS extension you use to optimize recursive resolution for query sources that are not topologically close to the recursive resolvers. When you enable ECS for recursive resolution, the appliance includes subnet information of the host that originates a DNS query. Thus, your recursive resolver can perform geotargeting by passing the subnet information to authoritative servers so that the response will be more optimized for the end clients. For example, when you enable ECS and/or ECS forwarding on your recursive resolver, CDNs (Content Delivery Networks) can deliver content faster and more efficiently to the end user by providing information about the end user's subnet to the authoritative DNS server operated by the CDNs.

You can enable the NIOS appliance to handle recursive queries using ECS option and enable ECS forwarding support at the Grid level. You can then add whitelisted zone names that are subject to ECS recursion and specify the source prefix length for IPv4 and IPv6 addresses. Make sure you enter only apex zones. Example: foo.com, corpxyz.com, etc. The whitelisted zone name indicates the zone to which ECS tagged queries must be sent.

Note the following while adding whitelisted zone names:

- ECS options are sent only when the name being queried and the apex of the zone being queried both match ECS zones. For example, if the zone "foo.com" contains a subdomain "www.foo.com", then you must configure "foo.com" as ECS zone and not "www.foo.com". The latter configuration might result in no ECS queries being sent, because the apex zone, "foo.com" does not match with "www.foo.com".
- Queries for subdomains of the specified zone name, with prefix lengths greater than the specified prefix length is not applicable for the subdomains of the specified zone name. For example, if you specify "foo.com" with IPv4 prefix length 20, then IPv4 queries with prefix length greater than 20 is not applicable for the subdomains of "foo.com".
- You can exclude certain subdomains by adding a leading exclamation mark (!) to the subdomain name. Example: ! foo.example.org, ! test.foo.com, etc.

Guidelines for Using ECS and ECS Forwarding

The following are the guidelines for using ECS and ECS forwarding:

- When recursive ECS is enabled, the appliance applies ECS handling for queries that meet both of the following criteria:
  - If the source prefix length is not set to zero.
  - If the query name matches one of the listed whitelisted zone names.
- If you enable ECS forwarding, all queries that contain a valid ECS option will be forwarded to the authoritative server.
- Queries with the source prefix length set to zero will be forwarded unchanged, regardless of whether ECS forwarding is enabled or disabled.
- When recursive ECS and ECS forwarding are enabled, then response to queries that contain a valid ECS option with a non-zero source prefix length will contain an ECS option.
- When recursive ECS is enabled and ECS forwarding is disabled, and if the original query contains a valid ECS option with a non-zero source prefix length, then the resolver returns a REFUSED response.

To enable recursive ECS and configure DNS resolver parameters, complete the following:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. In the Grid DNS Properties editor, click the Advanced subtab of the Queries tab and complete the following:
   - **Enable Recursive ECS**: Select this check box to enable recursive resolution using ECS. This is disabled by default. If recursive ECS is enabled, the appliance applies ECS handling for queries that meet both of the following criteria:
     - If the source prefix length is not set to zero.
     - If the query zone name is listed in the whitelisted domains.
   - **Enable ECS Forwarding**: Select this check box to enable ECS forwarding. If you enable ECS forwarding, all queries containing a valid ECS option will be forwarded to the authoritative server.

**Note**: Queries with the source prefix length set to zero will be forwarded unchanged, regardless of whether ECS forwarding is enabled or disabled.
Query Zone Permissions: Click the Add icon to add a list of query zone names that are subject to ECS recursion and the corresponding permission. Grid Manager adds a row to the table. Complete the following:
  - **Zone Name**: Enter the zone name.
  - **Permission**: Select **Allow** or **Deny** from the drop-down list.

IPv4SourcePrefix: Specify the IPv4 source prefix length. You can enter a value between 1 and 24. The default value is 24.

IPv6SourcePrefix: Specify the IPv6 source prefix length. You can enter a value between 1 and 56. The default value is 56.

### Enabling DNS Fault Tolerant Caching

When an authoritative DNS server experiences an outage, all the web sites served by the DNS server becomes inaccessible. Enabling the DNS fault tolerant caching option allows users to access the web sites served by the DNS server despite the DNS server outage. When you enable the DNS fault tolerant caching option, DNS records are retained in the recursive cache even after they expire. Whenever recursive query times out or returns a SERVFAIL response, the appliance returns the cached response to the client instead of the SERVFAIL response.

When you enable DNS fault tolerant cache, you can also specify the TTL (time-to-live) and timeout settings for the expired records. TTL specifies the time duration for which the expired record is retained in the recursive cache. Setting a high TTL might cause the client to use incorrect data for a longer duration. Conversely, setting a low TTL renders more current cached data, but also increases the traffic on your network. The expired record is deleted from the recursive cache after the specified timeout duration.

Only DNS members with recursion enabled can support this feature. You can enable this feature at the Grid level and override it at member level with recursion enabled. For information on enabling recursion for a Grid or member, see [Enabling Recursive Queries](#).

To enable DNS fault tolerant caching, complete the following:

1. **Grid**: From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Grid DNS Properties**. To override Grid settings, click **Override** next to it and complete the appropriate fields.

2. **Member**: From the **Data Management** tab, select the **DNS** tab and click the **Members** tab -> member check box -> **Edit** icon.

   - **Enable Fault Tolerant Caching**: Select this check box to enable the retention of expired records in the recursive cache. Whenever recursive queries times out or returns a SERVFAIL response, the appliance returns the cached response to the client instead of the SERVFAIL response. This is disabled by default.

   - **Expired Record TTL**: Specify the time duration that the appliance retains the expired records in the recursive cache. The default is five seconds. Select the time period in minutes, hours, or days from the drop-down list.

   - **Expired Record Timeout**: Specify the time duration that the appliance waits before deleting the expired records from the recursive cache. The default is 24 hours. Select the time period in minutes, hours, or days from the drop-down list.

3. Save the configuration.

### Controlling AAAA Records for IPv4 Clients

By default, the NIOS appliance returns resource records, including AAAA records, in response to DNS queries. You can enable the appliance to filter and remove AAAA records in response to queries received over IPv4 for each name server and DNS view. This feature is useful in a configuration where a client issues a DNS query over IPv4 when it does not have the ability to use an IPv6 address. When a response returns an IPv6 address however, the client that sends the query over an IPv4 transport would lose connectivity. By enabling AAAA filtering, you can configure your name server not to return AAAA records to clients that request queries over an IPv4 transport. Presumably, these clients then re-query the name server for A records for the same domain name.

Depending on your configuration, the appliance can remove AAAA records for all queries over IPv4 (even when DNSSEC is enabled), or only for queries that are not DNSSEC-signed. You can also create a list of IPv4 networks and addresses to which the appliance applies AAAA filtering and vice versa. You can enable and configure AAAA filtering for the Grid, members, and DNS views.

To control whether you want the appliance to return AAAA records for queries sent over IPv4, you must first enable AAAA filtering, and then create a list of IPv4 networks and addresses that allow or deny AAAA filtering from the appliance, as described in [Enabling AAAA Filtering](#).

**Note:** An AAAA record is filtered only when there is also an A record for the same domain name. In this case, the appliance still sends a response, but without any AAAA or A record in it. When a client queries for an AAAA record and there is no corresponding A record for it, the appliance returns the AAAA record even if you have enabled AAAA filtering for this client.

### Enabling AAAA Filtering

To enable AAAA filtering and configure a list of IPv4 networks and addresses:

1. **Grid**: From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Grid DNS Properties**. To override Grid settings, click **Override** next to it and complete the appropriate fields.

   **DNS View**: From the **Data Management** tab, select the **DNS** tab -> Members tab -> member check box -> **Edit** icon.

2. **Member**: From the **Data Management** tab, select the **DNS** tab -> Zones tab -> DNS View check box -> **Edit** icon.

To override Grid settings, click **Override** and complete the appropriate fields.

**Enable AAAA Filtering**: From the drop-down list, select one of the following:
• **Break DNSSEC**: Select this to remove AAAA records in response to queries sent over IPv4, including those that are signed by DNSSEC.

**Note**: Be aware that when you select this option, DNSSEC configuration will no longer be in effect.

• **No**: Select this to disable AAAA filtering for queries over IPv4. When you select this, the appliance returns AAAA records in response to all DNS queries over IPv4. This is selected by default.

• **Yes**: Select this to enable AAAA filtering for queries over IPv4. When you select this, the appliance removes AAAA records in response to all DNS queries issued over IPv4, except for DNSSEC-signed requests.

3. In the AAAA Filtering section, select one of the following:

• **None**: Select this if you do not want to configure access control for AAAA filtering. The appliance allows all clients to issue DNS queries over IPv4 when they do not have the ability to use IPv6 addresses. This is selected by default.

• **Named ACL**: Select this and click **Select Named ACL** to select a named ACL. Grid Manager displays the *Named ACLs Selecto*

• **Set of ACEs**: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows.

  - **IPv4 Address**: Select this to add an IPv4 address. Click the **Value** field and enter the IP address of the client. The **Permission** column displays **Allow** by default. You can change it to **Deny** by clicking the field and selecting **Deny** from the drop-down list. When you select **Allow**, the appliance applies AAAA filtering and removes AAAA records in response to queries sent by the specified IPv4 address. When you select **Deny**, the appliance does not apply AAAA filtering and thus returns AAAA records.

  - **IPv4 Network**: In the **Add IPv4 Network** panel, complete the following, and then click **Add** to add the network to the list:

    - **Address**: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.

    - **Permission**: Select **Allow** or **Deny** from the drop-down list.

• **Any Address/Network**: Select to allow or deny AAAA filtering from any IP addresses.

After you have added access control entries, you can do the following:

• Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL icon and enter a name in the **Convert to Named ACL** dialog box. The appliance creates a new named ACL and adds it to the **Named ACL** panel. Note that the ACEs you configure for this operation stay intact.

• Reorder the list of ACEs using the up and down arrows next to the table.

• Select an ACE and click the **Edit** icon to modify the entry.

• Select an ACE and click the **Delete** icon to delete the entry. You can select multiple ACEs for deletion.

**Note**: Note that if you do not enter any addresses or networks in the table, the appliance applies AAAA filtering to all IPv4 clients. In other words, the appliance removes AAAA records in responses to all queries sent over IPv4.

### About NXDOMAIN Redirection

When a DNS member with recursion enabled receives a recursive query for data for which it is not authoritative, it locates the data through queries to other servers. If the query is for a non-existent domain name, the DNS member receives an NXDOMAIN response from the authoritative name server, which the member then forwards to the DNS client. An NXDOMAIN response contains a “Name Error” RCODE, signifying that the domain name referenced in the query does not exist. (For information, you can refer to RFC 1035, Domain Names — Implementation and Specification.)

You can install a Query Redirection license on a recursive DNS member to control its response to queries for A records of non-existent domain names and other domain names that you specify. After the license is installed, Grid Manager displays the **NXDOMAIN Rulesets** tab where you can create rules that specify how a DNS member responds to queries for A/AAAA records for certain domain names and non-existent domain names. Each rule contains a domain name specification, and the action of the DNS member when the domain name in the query matches that in the rule. After you create the rules, you then enable the NXDOMAIN redirection feature and list the IP addresses that are included in the synthesized responses.

Recursive DNS members can redirect responses to queries for A/AAAA records only. DNS members resolve queries for all other records as they normally would. In addition, you can enable DNS members to log queries that match rules with an action of “Redirect” or “Modify”. You can view the logs in the **syslog viewer**. The logs include the queried domain name, source IP address, the pattern of the matched rule, and the name of the corresponding ruleset.

When DNSSEC is enabled on the Infoblox DNS server, it does not redirect DNS clients that request DNSSEC data for a non-existent domain name. Instead, it returns an authenticated negative response in the form of an NSEC or NSEC3 RR. (For information about DNSSEC, see Chapter 22, DNSSEC.) If DNSSEC is not enabled, the appliance ignores the request for DNSSEC data and redirects the clients.

To apply the configured NXDOMAIN rules regardless of whether a DNS query requests DNSSEC data, configure the appliance accordingly. For more information about how to configure this, see Applying Policies and Rules to DNS Queries that Request DNSSEC Data. You can enable NXDOMAIN redirection at the Grid, member, and DNS view levels. Only recursive DNS servers can redirect DNS clients. Non-recursive DNS members do not redirect DNS clients. For information on enabling recursion on a DNS member, see Enabling Recursive Queries.

Note that if both NXDOMAIN redirection and the blacklisting feature are enabled, the DNS member applies the blacklist rulesets before the NXDOMAIN rulesets. For information about blacklisting domain names, see About Blacklists.
About NXDOMAIN Rule Sets

An NXDOMAIN ruleset is a list of rules that a DNS member uses to determine its response to recursive queries for A records it does not have. Each rule consists of a domain name specification or pattern, and an associated action.

Domain names can contain any printable character. You can use certain metacharacters to create domain name patterns that are used to match the domain names in DNS queries. Pattern matching is case-insensitive. Patterns support the following metacharacters:

- **Use the caret character (`^`) to indicate the beginning of a pattern.** For example, `^foo` matches `foo.com` but not `barfoo.com`. The caret character has a special meaning only if it is specified at the beginning of a pattern.
- **Use the dollar sign character (`$`) to indicate the end of a pattern.** The dollar sign character has a special meaning, only if it is specified at the end of the pattern. For example, `com$` matches `corpxyz.com` but not `corpxyz.com.net`.

  When the pattern contains a `$` at the end, NIOS automatically adds a period (`.`) before the `$`. For example, if you enter `com$,` NIOS saves it as `.com.$`. The period indicates that the pattern specifies a complete domain name that ends with the root label.

- **Use the asterisk character (`*`) as a wildcard that can match zero or more characters in one or more labels of a domain name.** For example, `xf*oy` matches `xfooy.com`, but not `xfoobary`.

  A pattern that contains a single asterisk (`*`) (or an equivalent expression, such as `"^\*S\*"`) matches any domain name.

- **Use the backslash character (`\`) with one of the metacharacters (``, `^`, `*`, and `{}`).** To remove their special meaning. If `\` is followed by any other character, that character is taken as an ordinary character, as if `\` is not present. For example, `foo\bar` matches a literal asterisk in a domain name.

  No other characters have any special meaning. Note in particular that the period character (".") only matches a period used as a separator in a domain name.

The action specifies how the DNS member responds when a domain name in a query matches a pattern. The action can be one of the following:

- **Pass**: The DNS member resolves the query and forwards the response to the DNS client, even if it is an NXDOMAIN response.
- **Modify**: The DNS member resolves the query and forwards the response to the DNS client, only if it is not an NXDOMAIN response. But if the member receives an NXDOMAIN response, it sends the client a synthesized response that includes predefined IP addresses.
- **Redirect**: The DNS member does not resolve the query. Instead, it sends the client a synthesized response that includes predefined IP addresses.

You can configure multiple rulesets. The DNS member applies the rulesets and their rules in the order in which they're specified in the configuration. If multiple rulesets contain rules with duplicate patterns, the DNS member applies the first rule it encounters and ignores the other rules.

Examples

The following example illustrates how the appliance applies NXDOMAIN rulesets. Ruleset 1:

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>a1.corpxyz.com</td>
<td>PASS</td>
</tr>
<tr>
<td>*.corpxyz.com</td>
<td>REDIRECT</td>
</tr>
</tbody>
</table>

- If the DNS member receives a query for `a1.corpxyz.com`, it resolves the query and forwards the response, even if it is an NXDOMAIN response, to the client. Note that if the order of the rules was switched, the DNS client would have been redirected immediately, because the domain name `a1.corpxyz.com` matches the `*.corpxyz.com` pattern.

- If the DNS member receives a query for `b1.corpxyz.com`, the member immediately redirects the DNS client to the specified IP address because the domain name in the query matches the second rule.

- If the DNS member receives a query for `b1.corp200.com`, it resolves the query because the domain name does not match any rule. If the DNS member receives an A record from an authoritative server, the member forwards the response to the client. However, if the member receives an NXDOMAIN response, it redirects the DNS client to the specified IP address.

In the following example, the rules redirect queries for dotted domain names that do not have `*.com` As shown in the example, an explicit PASS rule is required at the end.

Ruleset 2:

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.com</td>
<td>PASS</td>
</tr>
<tr>
<td>.*$</td>
<td>MODIFY</td>
</tr>
<tr>
<td>*</td>
<td>PASS</td>
</tr>
</tbody>
</table>
- If the DNS member receives a query for corpxyz.com which matches the pattern "*.com", the member resolves the query and forwards the response, even if it is an NXDOMAIN response, to the client.
- If the DNS member receives a query for corpxyz.org, which matches the pattern ".*.$", the member resolves the query. If the member receives an NXDOMAIN response, it redirects the client to the specified IP address. If the member receives a non-NXDOMAIN response, it forwards the response to the client.
- If the DNS member receives a query for corp200, the member resolves the query and forwards the response to the client.

**NXDOMAIN Redirection Guidelines**

The following summarizes how a DNS member responds to a query for an A record when the NXDOMAIN feature is enabled:

- If there are no rulesets configured, the DNS member queries other name servers.
  - If the DNS member receives a non-NXDOMAIN response from an authoritative server, it forwards the response to the DNS client.
  - If the DNS member receives an NXDOMAIN response from an authoritative server, it redirect the DNS client.
- If rulesets are configured, the DNS member tries to match the domain name in the query with a domain name in the rules.
  - If the DNS member finds a match, it perform the action specified in the rule.
    - If the action is "Redirect", the DNS member redirect the DNS client.
    - If the action is "Pass", the DNS member queries other name servers and forwards the response to the DNS client.
    - If the action is "Modify", the DNS member queries other name servers. If it receives a non-NXDOMAIN response, it forwards the response to the DNS client; if it receives and NXDOMAIN response, it redirects the DNS client.
  - If the DNS member does not find a match, the DNS member queries other name servers.
    - If the DNS member receives a non-NXDOMAIN response, it forwards the response to the DNS client.
    - If the DNS member receives an NXDOMAIN response from an authoritative server, it redirects the DNS client.

Note that if an A record with a dotted hostname is added to an authoritative zone through a dynamic DNS update, and that A record should actually belong in an existing delegation, the appliance may not redirect a query for that A record according to the Blacklist and NXDOMAIN guidelines.

**Configuring NXDOMAIN Redirection**

To enable NXDOMAIN redirection and configure its properties:

1. Configure NXDOMAIN rulesets. You can create NXDOMAIN rulesets through Grid Manager, as described in *Creating Rulesets*. You can also specify the rulesets in a CSV file and import the file to the Grid, as described in *About CSV Import*.
2. Enable this feature and specify the redirection IP addresses, as described in *Enabling NXDOMAIN Redirection*.

**Creating Rulesets**

To create a ruleset:

1. From the Data Management tab -> DNS tab -> NXDOMAIN Rulesets tab, click the Add icon.
2. In the NXDOMAIN Ruleset wizard, complete the following and click Next:
   - **Name**: Enter a name for the ruleset.
   - **Comment**: You can enter additional information.
   - **Disable**: You can disable this ruleset for use later on. The appliance ignores disabled rulesets.
3. Click the Add icon to add a rule to the ruleset table.
   - In the Pattern column, enter a domain name or pattern, using the guidelines specified in *About NXDOMAIN Rulesets*.
   - In the **Action** column, select PASS, REDIRECT or MODIFY.
   - In the Order column, NIOS automatically displays the number of the entry in the list.
   - The appliance applies the rules in the order they are listed. You can order the list as follows:
     - Use the up and down arrows to move rules up or down on the list.
     - Use the go-to-top or go-to-bottom arrow to move a rule to the top or bottom of the list.
     - Change the Order number of a rule to move it to the desired location.
     - Delete a rule by selecting it and clicking the Delete icon.
4. Save the configuration and click **Restart** if it appears at the top of the screen.

**Managing NXDOMAIN Rulesets**

To view NXDOMAIN rulesets, navigate to the Data Management tab -> DNS tab -> NXDOMAIN Rulesets tab. The panel lists the configured rulesets and their associated comments. You can also display the Disabled column which indicates which rulesets are disabled. From this panel, you can do the following:

- Add more rulesets, as described in the preceding section, *Creating Rulesets*.
- Edit a ruleset, by clicking its check box and clicking the Edit icon. You can set the following in the NXDOMAIN Ruleset editor:
  - In the General Basic tab, you can change entries in any of the fields.
  - In the Rules tab, you can do the following:
• Add a rule by clicking the add icon and specifying the pattern and action.
• Change the pattern or action of a rule, by clicking in the appropriate row.
• Delete a rule by clicking its check box and clicking the Delete icon.
• Move rules up and down, by using the arrows.
• In the Permissions tab, you can set admin permissions for the ruleset. For information about admin permissions, see Chapter 4, Managing Administrators.
• Delete a ruleset, by clicking its check box and clicking the Delete icon.

Enabling NXDOMAIN Redirection

Only DNS members with recursion enabled can support NXDOMAIN redirection.
You can enable this feature at the Grid level, and override it for a member or DNS view with recursion enabled. You must specify at least one IP address as the redirection destination. You can specify different redirection IP addresses and rulesets for each Grid member or DNS view, and you can also define members that do not provide redirection. This is useful when you want to define a set of "opt out" servers for DNS clients that do not want to be redirected.
You can also enable the DNS member to log queries that match rules with an action of "Redirect" or "Modify". The logs include the queried domain name, source IP address, the pattern of the matched rule, and the name of the corresponding ruleset. The DNS member does not log queries that matched rules with an action of "Pass".
To enable NXDOMAIN redirection:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   Member: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
   DNS View: From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view check box -> Edit icon.
   Standalone DNS: From the Data Management tab, select the DNS tab, expand the Toolbar and click System DNS Properties.
   To override an inherited property, click Override next to it and complete the appropriate fields.
2. If the Grid DNS Properties or Member DNS Properties editor is in basic mode, click Toggle Advanced Mode.
3. Click NXDOMAIN and complete the following:
   • Enable NXDOMAIN redirection (recursive members only): Select this option to enable recursive DNS members to synthesize their responses to DNS queries for A records.
   • Rulesets: Click the Add icon to add an NXDOMAIN ruleset. Use the up and down arrows to move rulesets up and down in the list. The appliance applies them in the order they are listed.
   • Redirect to IPv4 addresses: Click the Add icon and enter the IPv4 addresses that the DNS server includes in its synthesized response for A type queries.
   • Redirect to IPv6 addresses: Click the Add icon and enter the IPv6 addresses that the DNS server includes in its synthesized response for AAAA type queries.
   
   Note: You can add up to 12 IP addresses, combination of both IPv4 and IPv6, for NXDOMAIN redirection.

   • TTL: Specify how long the DNS client caches the A record with the redirected IP address.
   • Log redirected queries: Select this check box to log the redirected queries to syslog.
4. Save the configuration and click Restart if it appears at the top of the screen.

Detecting and Mitigating DNS DDoS Attacks

DNS is a tempting target for attacks given that most traditional enterprise firewalls are configured to allow port 53 traffic to service DNS, which gives attackers an easy way to evade your firewall implementation. Since DNS queries are asymmetrical, they can result in a response many times larger than the query, which means that your DNS system can be used to amplify an attack.
To protect your DNS servers and DNS service performance, Infoblox provides the following features to detect and mitigate DNS DDoS attacks, such as NXDOMAIN attacks:

• Automated mitigation of phantom domain attacks (a subset of NXDOMAIN attacks), as described in Automated Mitigation of Phantom Do
  main Attacks.
• Configurable parameters used to detect possible NXDOMAIN attacks, as described in Detecting NXDOMAIN Attacks.
• Mitigation of NXDOMAIN responses by removing the LRU (Least Recently Used) items from the list of NX (non-existent) RRsets. The appliance uses the LRU list to select entries for removal from the cache when the cache utilization exceeds the allowed threshold. For more information, see Mitigating Possible NXDOMAIN Attacks.
• CLI commands for configuring RRL (Response Rate Limiting) to mitigate DNS DDoS attacks by reducing the rate at which authoritative servers respond to high volumes of malicious queries, as described in Support for RRL (Response Rate Limiting).

Infoblox also offers the following security features to fully protect your DNS infrastructure and implementation:

• Infoblox Advanced DNS Protection
• Infoblox DNS Firewall
• Infoblox Threat Insight

Automated Mitigation of Phantom Domain Attacks

A phantom domain attack happens when the attacker sets up "phantom" domains that do not respond to DNS queries. Under normal circumstances, the DNS recursive server contacts authoritative servers to resolve recursive queries. When phantom domain attacks happen, the recursive server continues to query non-responsive servers, which causes the recursive server to spend valuable resources waiting for responses. When resources are fully consumed, the DNS recursive server may drop legitimate queries, causing serious performance issues.
NIOS provides a few configurable parameters for mitigating phantom domain attacks in which recursive server continues to query non-responsive servers. Before you configure any of the parameters for mitigating phantom domain attacks, review the guidelines that might help you understand the relationship between these parameters. For information, see Guidelines for Mitigating Phantom Domain Attacks.

To configure parameters for mitigating phantom domain attacks, see Configuring Parameters for Mitigating Phantom Domain Attacks. All events related to these operations are logged to the syslog. For information about the syslog and how to use it, see Using a Syslog Server.

Guidelines for Mitigating Phantom Domain Attacks

To detect phantom domain attacks, you can review your log messages. One possible indication of attack is when you receive a log message similar to the following:

```
2015-04-29T10:20:06+00:00 daemon infoblox named[25390]: warning no more recursive clients: quota reached
```

Consider the following guidelines to mitigate the attack:

- Increase the number of recursive clients.
- Use a combination of the following parameters to achieve optimum results:
  - Limit recursive queries per server and Limit recursive queries per zone
  - Enable hold down for non-responsive servers and Limit recursive queries per zone
  - When you enable any of the options, the default values are set at an optimum level for general operations. Infoblox recommends that you keep the default values when using these commands. Ensure that you understand the ramifications if you want to change the default values.

Configuring Parameters for Mitigating Phantom Domain Attacks

Note: Changes made to the configuration for mitigating phantom domain attacks take effect immediately on active DNS service and do not require a service restart.

To adjust the parameters to mitigate phantom domain attack parameters, complete the following:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. **Member**: From the Data Management tab -> Members tab -> member check box -> Edit icon. To override Grid settings, click Override and complete the appropriate fields.

2. In the Grid DNS Properties or Member DNS Properties editor, click the Security tab and complete the following in the Non-responsive servers section:

- **Enable hold down for non-responsive servers**: When you select this check box, the appliance stops sending queries to non-responsive servers for a specified time interval (Hold down duration) when the number of consecutive attempts to contact a non-responsive server exceeds the threshold value (Timeouts to trigger). No service restart is required when you change this. Clear this check box to disable the hold down. Note that disabling this does not clear any of the previously configured values. When you enable this feature again, the appliance preserves the previously configured values.
  - **Minimum timeout**: When the time taken for a timeout to happen exceeds this number, the timeout is counted towards the number of consecutive timeouts (Timeouts to trigger). You can specify a value between 0 and 5000 milliseconds. For example, if you set the minimum timeout to 1000 milliseconds, only timeouts that took longer than 1000 milliseconds are counted towards the number of consecutive timeouts. The default is 1000 milliseconds.
  - **Timeouts to trigger**: The number of consecutive timeouts before holding down a server. You can specify a value between 0 and 4294967295. For example, setting the threshold value to 5 means the appliance stops sending queries to the non-responsive server after five consecutive timeouts. The default is 5.
  - **Hold down duration**: The hold down duration for a server. You can specify a value between 1 and 86400 seconds. For example, if you set the hold down time to 60 seconds, the server stops sending queries for 60 seconds. The default is 60 seconds.

Note: In order to get enough upstream queries and for the appliance to effectively identify non-responsive servers and stop sending queries to them, do not set a high value for the Minimum timeout field. The higher the value you configure for this field, the longer it takes to capture a timeout and the harder it is to satisfy the total counts of consecutive timeouts (Timeouts to trigger). Until the total count of consecutive timeouts is exceeded, no mitigation happens against the non-responsive servers. As a result, it is less likely for the appliance to identify phantom domain attacks when you set the Minimum timeout field at a high value. Infoblox highly recommends that you keep the default Minimum timeout value to achieve optimum protection against these attacks.

- **Limit recursive queries per server**: Select this check box to configure the maximum number of concurrent recursive queries that the appliance sends to a single upstream name server. Queries above the limit will be blocked and may result in a SERVFAIL response to the client. When you enable this option, the appliance dynamically adjusts the concurrent query limit for a specific server based on the ATR (Average Timeout Ratio). No service restart is required when you change this. Clear this check box to disable this option. Note that disabling this does not clear any of the previously configured values. When you enable this feature again, the appliance preserves the previously configured values.
  - **Maximum fetches per server**: The maximum number of concurrent recursive queries that the appliance sends to a single upstream name server before blocking additional queries to that server. You can specify a value between 0 and 4294967295. The default value is 500.
• **Quota recalculation interval:** This determines how often (in number of recursive responses) the appliance recalculates the average timeout ratio. You can specify a value between 0 and 4294967295. The default value is 200. Note that if you set this value to 0 (zero), the appliance will never re-calculate the ATR. Infoblox strongly recommends that you do not set this value to 0.

• **Limit recursive queries per zone:** Select this check box to configure the maximum number of concurrent recursive queries the DNS server sends for a domain. If the number of recursive queries exceeds the configured value, the server blocks new queries for that domain and returns a SERVFAIL response to the client. No service restart is required when you change this. Clear this check box to disable the option. Note that disabling this does not clear any of the previously configured values. When you enable this feature again, the appliance preserves the previously configured values.

  • **Maximum fetches per zone:** The maximum number of concurrent recursive queries that a server sends for one of its domain. When the number of queries exceeds this number, the server blocks new queries for the domain. You can specify a value between 0 and 4294967295. The default value is 200

### Detecting NXDOMAIN Attacks

NXDOMAIN attacks are symmetrical DoS attacks that involve a large number of DNS clients sending queries for invalid or non-existent domains, which results in DNS recursion and NXDOMAIN responses. As a result, the DNS server spends valuable resources processing spurious requests instead of providing legitimate DNS services. When a DNS server is under NXDOMAIN attack, clients cannot get valid responses because the cache of the DNS server is flooded with NXDOMAIN results.

Infoblox provides a few options for detecting possible NXDOMAIN attacks. You can track one or all of the following to raise alerts for these attacks:

- High percentage of NXDOMAIN responses, as described in Tracking NXDOMAIN Responses.
- Low cache hit ratio for queries, as described in Tracking Cache Hit Ratio of Recursive Queries.
- High number of dropped UDP packets, as described in Tracking Dropped UDP Packets.

Each of these options provides configurable parameters that determine if an alert should be raised. When an alert is triggered, the appliance sends SNMP traps about possible NXDOMAIN attacks. All triggered events are logged to the syslog. Note that you must enable notifications in order for the appliance to send SNMP traps. For more information about how to enable this, see Setting SNMP and Email Notifications.

**Note:** The default values for these configurable parameters are set at an optimum level for general operations. Infoblox recommends that you keep the default values when using these features. Ensure that you understand the ramifications if you want to change the default values.

### Tracking NXDOMAIN Responses

When under NXDOMAIN attack, the ratio of NXDOMAIN responses from upstream servers to all incoming recursive responses is typically high. When the ratio of NXDOMAIN responses to all incoming recursive responses exceeds the configured high water threshold, the appliance sends an alert. Note that timeouts are not counted as responses for this detection.

**Note:** Changes made to the configuration for tracking NXDOMAIN responses take effect immediately on active DNS service and do not require a service restart.

To configure the parameters for tracking NXDOMAIN responses, complete the following:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. **Member:** From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon. To override Grid settings, click Override and complete the appropriate fields.

2. **In the Grid DNS Properties or Member DNS Properties editor,** click the Security tab and complete the following in the Bogus-query alerting and mitigation section:

   - **Track the percentage of NXDOMAIN responses to recursive queries:** Select this check box to track the percentage of NXDOMAIN responses from upstream servers to all incoming recursive responses. Clear this check box to disable the detection. Note that disabling this does not clear any of the previously configured values. When you enable this feature again, the appliance preserves the previously configured values. This is selected by default.

   - **Minimum responses per interval:** Enter the minimum number of incoming DNS responses received (within the detection interval) before the appliance starts calculating the NXDOMAIN ratio at the end of the detection interval. The appliance then compares the calculated percentage to the high water threshold. If the percentage equals or exceeds the high water threshold, the appliance sends an SNMP trap (if enabled) about possible NXDOMAIN attacks. The default is 1000. Note that the Minimum responses per interval is implemented to ensure that enough incoming DNS responses are received so the appliance can calculate a meaningful NXDOMAIN ratio and does not declare possible attacks from a small response sample. Therefore, when you change the default value, ensure that you use a reasonable value so the appliance calculates the NXDOMAIN ratio from a reasonable amount of responses. Raising an alert using a small response sample may not be a reliable way for detecting possible NXDOMAIN attacks.

   - **NXDOMAIN threshold:** Enter the Low and High water thresholds at which an alert is triggered. The appliance sends an alert when the percentage equals or exceeds the High water threshold. When the percentage in subsequent detection intervals falls below the Low water threshold, the appliance sends another alert to notify that the percentage of NXDOMAIN responses has gone back to an acceptable level. The defaults are 70% for Low and 80% for High.

   - **Detection interval and Responses:** These parameters work as alternatives to each other in determining when the appliance starts calculating the NXDOMAIN ratio. In the case of a very low response rate when the total responses
Configuration Examples for Tracking NXDOMAIN Responses

The following examples demonstrate how different responses per second affect the calculation of NXDOMAIN ratio.

**Example One: Total responses per second = 250 and parameters = default values**

<table>
<thead>
<tr>
<th>Detection Interval (10 seconds)</th>
<th>Total Responses per Second</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
<th>6th</th>
<th>7th</th>
<th>8th</th>
<th>9th</th>
<th>10th</th>
</tr>
</thead>
<tbody>
<tr>
<td>250/s</td>
<td></td>
<td>0</td>
<td>250</td>
<td>500</td>
<td>750</td>
<td>1000</td>
<td>1250</td>
<td>1500</td>
<td>1750</td>
<td>2000</td>
<td>2250</td>
</tr>
</tbody>
</table>

In this example, the total number of responses is 250 per second and the total number of responses hits the Minimum responses per interval (default = 1000) at the 4th second of the detection interval. This meets the requirement for the Minimum responses per interval and triggers an NXDOMAIN ratio calculation at the end of the detection interval (default = 10 seconds). If the percentage equals or exceeds the high water threshold, the appliance sends an alert and logs the event to the syslog to notify about possible NXDOMAIN flood attacks. The appliance resets the response counters for the next detection interval.

**Example Two: Total responses per second = 40 per second and parameters = default values**

<table>
<thead>
<tr>
<th>1st Detection Interval (10 seconds)</th>
<th>Total Responses per Second</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
<th>6th</th>
<th>7th</th>
<th>8th</th>
<th>9th</th>
<th>10th</th>
</tr>
</thead>
<tbody>
<tr>
<td>40/s</td>
<td></td>
<td>0</td>
<td>40</td>
<td>80</td>
<td>120</td>
<td>160</td>
<td>200</td>
<td>240</td>
<td>280</td>
<td>320</td>
<td>360</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2nd Detection Interval (10 seconds)</th>
<th>Total Responses per Second</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
<th>6th</th>
<th>7th</th>
<th>8th</th>
<th>9th</th>
<th>10th</th>
</tr>
</thead>
<tbody>
<tr>
<td>40/s</td>
<td></td>
<td>440</td>
<td>480</td>
<td>520</td>
<td>560</td>
<td>600</td>
<td>640</td>
<td>680</td>
<td>720</td>
<td>760</td>
<td>800</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3rd Detection Interval (10 seconds)</th>
<th>Total Responses per Second</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
<th>6th</th>
<th>7th</th>
<th>8th</th>
<th>9th</th>
<th>10th</th>
</tr>
</thead>
<tbody>
<tr>
<td>40/s</td>
<td></td>
<td>840</td>
<td>880</td>
<td>920</td>
<td>960</td>
<td>1000</td>
<td>1040</td>
<td>1080</td>
<td>1120</td>
<td>1160</td>
<td>1200</td>
</tr>
</tbody>
</table>

In this example, the total number of responses per second is 40 per second. During the first detection interval of 10 seconds, the total number of responses is 400, which does not reach the Minimum responses per interval (default = 1000); therefore, no NXDOMAIN ratio calculation occurs and the response counters continue to accumulate into the second detection interval. At the end of the second interval, the total number of responses still does not reach the Minimum responses per interval; therefore, no NXDOMAIN ratio calculation occurs and the counters continue to accumulate. Finally, the total number of responses meets the requirement of the Minimum responses per interval when the appliance receives 1000 responses at the 5th second during the third detection interval. This triggers an NXDOMAIN ratio calculation at the end of the third detection interval, and the counters reset for the next detection interval. If the NXDOMAIN percentage equals or exceeds the high water threshold, the appliance sends an alert and logs the event to the syslog to notify about possible NXDOMAIN flood attacks.

**Example Three: Total responses per second = 50000 and parameters = default values**

<table>
<thead>
<tr>
<th>Detection Interval (10 seconds)</th>
<th>Total Responses per Second</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
<th>6th</th>
<th>7th</th>
<th>8th</th>
<th>9th</th>
<th>10th</th>
</tr>
</thead>
<tbody>
<tr>
<td>50000</td>
<td></td>
<td>0</td>
<td>50000</td>
<td>100000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In this example, the total number of responses per second is 50000. When the total number of responses hits 100000, which equals to the Response...
**Tracking Cache Hit Ratio of Recursive Queries**

Another way to track possible DNS attacks is to monitor the cache hit ratio of recursive queries. A cache hit means the response to a query can be found in the cache of the DNS server. When the response cannot be found, it is a miss. Cache hit ratio is the percentage of cache hits to the total number of queries. The higher the ratio, the more efficiently the cache is operating. When a server is under NXDOMAIN attack, the cache hit ratio tends to drop.

To track cache hit ratio, complete the following:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. **Member:** From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon. To override Grid settings, click Override and complete the appropriate fields.

2. In the Grid DNS Properties or Member DNS Properties editor, click the Security tab and complete the following in the Bogus-query alerting and mitigation section:
   - **Track the cache hit ratio of queries:** Select this check box to track the cache hit ratio of recursive queries. Clear this check box to disable the detection. No service restart is required when you change this. Note that disabling this does not clear any of the previously configured values. When you enable this feature again, the appliance preserves the previously configured values. This is selected by default.
   - **Minimum queries per interval:** Enter the minimum number of incoming DNS queries received (within the detection interval) before the appliance starts calculating the cache hit ratio at the end of the detection interval. The appliance then compares the calculated percentage to the low water threshold. If the percentage equals or falls below the low water threshold, the appliance sends an SNMP trap (if enabled) about possible NXDOMAIN attacks. The default is 1000. Note that the **Minimum responses per interval** is implemented to ensure that enough incoming DNS queries are received so the appliance can calculate a meaningful cache hit ratio and does not declare possible attacks from a small number of incoming queries. When you change the default value, ensure that you use a number that is big enough so the appliance calculates the cache hit ratio from a reasonable amount of queries.
   - **Minimum cache utilization:** Cache hit ratio detection does not start until cache utilization hits this number. In other words, the appliance does not calculate the cache hit ratio until the cache utilization has reached or exceeded this number. The default is 75%.

3. **Hit ratio threshold:** Enter the Low and High thresholds at which an alert is triggered. The appliance sends an alert when the cache hit percentage equals or drops below the Low water threshold, which means the cache hit rate is low enough that the server is not operating efficiently, and there could be a high number of bogus queries that do not have matching responses in the cache. When the cache hit percentage in subsequent detection intervals reaches or exceeds the High water threshold, the appliance sends another alert to notify that the cache hit rate has gone back to an acceptable level. The defaults are 70% for Low and 80% for High.

4. **Hit ratio detection interval** and **Responses:** These parameters work as alternatives to each other in determining when the appliance starts calculating the cache hit ratio. In the case of a very low response rate when the total responses received within the Hit ratio detection interval never reach the Minimum queries per interval, the response counters continue to accumulate into subsequent detection intervals until the Minimum queries per interval is met. The appliance then sends an alert at the end of the detection interval. On the other hand, in the case of a very high response rate when the total number of responses received equals or exceeds the Responses value before the Hit ratio detection interval is reached, the Minimum queries per interval does not apply and the appliance sends an alert as soon as the total responses equal or exceed the Responses value you define here. It does not wait till the end of the Hit ration detection interval. Note that the number of Responses you define here must be the same or greater than the Minimum queries per interval. The defaults are 10 seconds for the Hit ratio detection interval and 100000 for Responses.

3. Save the configuration.

**Tracking Dropped UDP Packets**

When the DNS server starts dropping UDP packets from incoming traffic, it can be an indication of DNS attacks. Tracking dropped UDP packets can help raise awareness of possible DDoS attacks. For these features, the appliance tracks all UDP packets, not only DNS queries. When tracking dropped UDP packets, the appliance tracks IPv4 and IPv6 packets independently.

To track dropped UDP packets, complete the following:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. **Member:** From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon. To override Grid settings, click Override and complete the appropriate fields.

2. In the Grid DNS Properties or Member DNS Properties editor, click the Security tab and complete the following in the Bogus-query alerting and mitigation section:
   - **Track the number of UDP packets dropped:** Select this check box to track the number of dropped UDP packets. Clear this check box to disable the detection. No service restart is required when you change this. Note that disabling this does not clear any of the previously configured values. When you enable this feature again, the appliance preserves the previously configured values.

Copyright ©2019, Infoblox, Inc. All right reserved.
Mitigating Possible NXDOMAIN Attacks

To mitigate possible NXDOMAIN attacks, you can configure the appliance to split the LRU (Least Recently Used) list into two: one for NX (non-existent) RRsets and the other for all other RRsets. The LRU list is used to select entries that the appliance removes from the cache when the cache utilization exceeds the allowed threshold, which is a fraction of the configured maximum cache size.

While this option is enabled, the appliance removes the least recently used items from the LRU list for NX RRsets before removing items from the LRU list for other RRsets. Doing so helps preserve valid DNS responses in the cache while eliminating NXDOMAIN responses.

To mitigate NXDOMAIN responses, complete the following:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. **Member**: From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon. To override Grid settings, click Override and complete the appropriate fields.

2. **In the Grid DNS Properties or Member DNS Properties editor**, click the Security tab and complete the following in the Bogus-query alerting and mitigation section:
   - **Deprioritize caching of NXDOMAIN responses**: Select this check box to split the LRU list into two: one for NX RRsets and the other for all other RRsets, and to always remove the least recently used items from the list of NX RRsets first. This is selected by default.

3. **Save the configuration.**

Support for RRL (Response Rate Limiting)

RRL provides the ability to control excessive UDP responses that are identical or almost identical. For more information about how RRL works, refer to the BIND Administrators Reference Manual at https://www.isc.org/downloads/bind/doc.

You can configure parameters for this feature through the following CLI commands: set dns_rrl and show dns_rrl. For more information about these commands, refer to the Infoblox CLI Guide.

You can also log RRL events to the syslog. To enable RRL logging, select rate-limit in the Logging Category when you configure logging for the Grid or member. For more information about how to select logging categories, see Setting DNS Logging Categories.

About Blacklists

Your organization can prevent customers or employees from accessing certain Internet resources, particularly web sites, by prohibiting a recursive DNS member from resolving queries for domain names that you specify.

You can create blacklist rules that specify how a DNS member responds to recursive queries for data for which it is not authoritative. Each rule specifies a domain name and the action of the DNS member when the domain name in the query matches that in the rule. Instead of resolving the query, the DNS member can redirect the DNS client to predefined IP addresses or return a REFUSED response code indicating that resolution is not performed because of local policy.

When the DNS member receives a query for data for which it is not authoritative, it first tries to match the domain name in the query with a domain name in any of its rules. If it finds a match, it responds according to the action specified in the rule. If it does not find a match and the NXDOMAIN feature is enabled, the DNS member checks the NXDOMAIN rulesets for a match and responds accordingly. If the NXDOMAIN feature is not enabled, the DNS member resolves the query. (For information about the NXDOMAIN feature, see About NXDOMAIN Redirection. Infoblox DNS members can modify their responses to queries for A records only. Therefore, if the matched query is for a record other than an A record, including a query with a type of "ANY", the DNS member sends a REFUSED response if the matched rule has an action of "Redirect".

In Figure 17.1, a DNS client opens a web browser and tries to access xxx.domain.com. When the DNS member receives the query for xxx.domain.com, it checks its blacklist rulesets and finds xxx.domain.com in a rule with an action of "Redirect". The DNS client is redirected to the configured redirection destination IP address 10.1.2.3.

---

Figure 17.1 Blacklist
This feature supports queries for data in IPv4 and IPv6 reverse-mapping zones, as well as forward-mapping zones. Note that when a user with a Windows DNS client with IPv6 installed tries to access a domain name, the Windows client sends queries for AAAA records before queries for A records. After the DNS member sends a Refused response to the query for the AAAA record, the DNS client then sends a query for the A record. The DNS member then responds according to the blacklist rules.

When DNSSEC is enabled on the Infoblox DNS server, it does not redirect DNS clients that request DNSSEC data. (For information about DNSSEC, see Chapter 22, DNSSEC.) If DNSSEC is not enabled and the query includes a request for DNS data, the appliance ignores the request for DNSSEC data and redirects the clients.

To apply the configured DNS blacklist rules regardless of whether a DNS query requests DNSSEC data, configure the appliance accordingly. For more information about how to configure this, see Applying Policies and Rules to DNS Queries that Request DNSSEC Data.

You can enable the blacklist feature at the Grid, member, and DNS view levels. Note that only recursive DNS servers can support this feature. For information on enabling recursion on a DNS member, see Enabling Recursive Queries.

### About Blacklist Rulesets

A blacklist ruleset is a list of rules that a DNS member uses to determine its response to recursive queries for certain domain names. When you enable the blacklist feature, you must define at least one rule in a ruleset. Each rule consists of a domain name and an associated action. The DNS member matches the domain names in the rules with the entire domain name in the query, including its suffix. The domain name in the rule can contain any printable character. Domain name matching is case-insensitive. Unlike the NXDOMAIN rules, blacklist rules do not support metacharacters in domain names.

The action in a rule is either "Pass" or "Redirect".

- **Pass**: The DNS member resolves the query and forwards the response to the DNS client.
- **Redirect**: The DNS member does not resolve the query. The DNS member redirects the client to the predefined IP addresses or sends a REFUSED response, depending on your configuration. Note that the DNS member can redirect the client only if the query is for an A record. If the query is for another resource record, the DNS member sends a REFUSED response.

You can use the Blacklist wizard, described in Adding a Blacklist Ruleset, to add blacklist rulesets, but not rules. You can only add rules by importing them in a CSV file, as described in About CSV Import. Note that if a blacklist ruleset contains duplicate domain names, the DNS member loads the first rule in the ruleset and discards the other rules.

The following example illustrates how the DNS member applies blacklist rules. Ruleset 1:

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>a1.foo.com</td>
<td>PASS</td>
</tr>
<tr>
<td>foo.com</td>
<td>REDIRECT/BLOCK</td>
</tr>
</tbody>
</table>

- If the DNS member receives a recursive query for a1.foo.com, it resolves the query and forwards the response to the client.
- If the DNS member receives a recursive query for the A record of b1.foo.com, it redirects the DNS client to the specified IP address. If the query is for another record type, such as an MX record, the member sends a REFUSED response to the client.

### Blacklist Guidelines
The following summarizes how a DNS member responds to a DNS client when the blacklist feature is enabled:

- If the domain name in the query matches a domain name in a rule, the member does the following:
  - If the query is for an A record, the member performs the action specified in the rule.
    - If the action is "Redirect", the member performs the action specified in the Blacklist wizard.
      - If the action in the wizard is to redirect, the DNS member redirects the client to the listed IP addresses.
      - If the action in the wizard is to return a REFUSED response, the DNS member sends a REFUSED response to the DNS client.
    - If the action in the rule is "Pass", the DNS member resolves the query and forwards the response to the DNS client.
  - If the query is for a non-A record, the member performs the action in the rule as follows:
    - If the action is "Redirect", the DNS member returns a REFUSED response to the DNS client.
    - If the action is "Pass", the DNS member resolves the query and forwards the response to the DNS client.

- If the domain name in the query does not match a domain name in a rule:
  - If the NXDOMAIN feature is enabled, the DNS member tries to find a match with the NXDOMAIN rules and responds accordingly.
  - If the NXDOMAIN feature is disabled, the DNS member resolves the query and forwards the response to the DNS client.

Note that if an A record with a dotted hostname is added to an authoritative zone through a dynamic DNS update, and that A record should actually belong in an existing delegation, the appliance may not redirect a query for that A record according to the Blacklist and NXDOMAIN guidelines.

Configuring the Blacklist Feature

To configure the blacklist feature:

1. Add blacklist rulesets, as described in Adding a Blacklist Ruleset.
2. Create one or more CSV files that contain the rules for each ruleset and import the files to the Grid. For information about importing CSV files, see About CSV Import.
3. Enable blacklisting, as described in Enabling Blacklisting.

Adding a Blacklist Ruleset

To add the name of a blacklist ruleset:

1. From the Data Management tab -> DNS tab -> Blacklist Rulesets tab, click the Add icon.
2. In the Blacklist wizard, complete the following:
   - Name: Enter a name for the ruleset.
   - Comment: You can enter additional information.
   - Disable: You can disable this ruleset for use later on. The appliance ignores disabled rulesets.
3. Save the configuration and click Restart if it appears at the top of the screen. You can then use the CSV Import feature to import the rules for each ruleset.

Managing Blacklist Rulesets

To view rulesets, navigate to the Data Management tab -> DNS tab -> Blacklist Rulesets tab. The panel lists the configured rulesets and their associated comments. You can also display the Disabled column which indicates which rulesets are disabled. From this panel, you can do the following:

- Add more rulesets, as described in the preceding section, Adding a Blacklist Ruleset.
- Edit a ruleset, by clicking its check box and clicking the Edit icon. You can set the following in the Blacklist Ruleset editor:
  - In the General Basic tab, you can change entries in any of the fields.
  - In the Permissions tab, you can set admin permissions for the ruleset.
- Delete a ruleset, by clicking its check box and clicking the Delete icon.
- View the rules that were imported in each ruleset by selecting it. For each rule, the panel displays the following:
  - Domain name
  - The action of the recursive DNS member when the domain name in a query matches the domain name in the rule.

To delete or edit rules in a ruleset, you must delete the ruleset from this panel, edit the CSV file and re-import it.

Enabling Blacklisting

Only DNS members with recursion enabled can support this feature. You can enable this feature at the Grid level and override it for a member or DNS view with recursion enabled.

You can also enable the DNS member to log queries that matched blacklist rules. The logs include the queried domain name, source IP address, the pattern of the matched rule, and the name of the corresponding ruleset.

To enable blacklisting:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
To configure zone transfers, you identify the servers to which zone data is transferred and optionally, servers to which data must not be transferred. For example, you can allow transfers to a network, but not to a specific server in the network. You can specify a different set of servers for specific Grid members and zones. For example, if certain Grid members are primary servers for a zone, then you can specify the secondary servers to which that member is allowed to transfer zones. You can also enable the appliance to add all IPv4 and IPv6 addresses for which you allow zone transfers to a zone data. You can configure this value to optimize the query rate on the network. In addition, when you have set up a few secondary name servers for a large number of zones, a delay in zone transfers may occur due to the default zone transfer configuration that limits concurrent zone transfers to 10 per secondary server. You can configure the maximum value of concurrent zone transfers to optimize the zone transfer operation. For information about how to optimize zone transfers, see Configuring Concurrent Zone Transfers.

Keep in mind that a database replication updates zone data for both the active and passive nodes of an HA member. Therefore, if there is a failover, the new active node (the previous passive node) immediately begins serving zone data with fresh information. In the case of a zone transfer, the passive node does not receive zone data until after a failover, when it becomes an HA master. At that time, it performs a zone transfer. If there is a lot of zone data, the transfer can take up to several minutes, thereby causing a break in the availability of the new HA master.

If you have Grid members as secondary servers, zone transfers can result in service interruption when there is a failover. Furthermore, if the primary server is down when the HA member fails over, the new active node cannot receive zone data until the primary server comes back online. You can use TSIG (transaction signature) keys to authenticate zone transfer requests and replies. The same key name and key value must be on the primary and secondary name servers for TSIG-authenticated zone transfers to occur. When using TSIG, it is important that both appliances involved in the authentication procedure use NTP (Network Time Protocol) for their time settings (see Using NTP for Time Settings). You can control zone transfers at the Grid member, and zone levels. This enables you to specify a different set of name servers for a Grid, member, and zone, if necessary. You can also control which external secondary servers should receive notifications about zone updates by adding their IP addresses to the also-notify statement for each authoritative zone that is served by a Grid member. Infoblox recommends that you use this feature to notify hidden external secondary servers about zone updates, instead of putting them in stealth mode, especially when you plan to configure a large number of them. For information about how to add IP addresses to the also-notify statement, see Configuring Zone Transfers.
2. In the editor, click Toggle Advanced Mode, select the Zone Transfers tab.
3. In the Allow zone transfers to section, select one of the following:
   - None: Select this to deny all clients for DNS zone transfers. This is selected by default.
   - Named ACL: Select this and click Select Named ACL to select a named ACL. Grid Manager displays the Named ACLs Selecto r. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this, the appliance allows remote name servers that have the Allow permission to send and receive zone transfer data. You can click Clear to select the named ACL.
   - Set of ACEs: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows.
     - IPv4 Address and IPv6 Address: Select this to add an IPv4 address or IPv6 address. Click the Value field and enter the IP address of the remote name server. The Permission column displays Allow by default. You can change it to Den y by clicking the field and selecting Deny from the drop-down list.
     - IPv4 Network: In the Add IPv4 Network panel, complete the following, and then click Add to add to the network to the list:
       - Address: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
       - Permission: Select Allow or Deny from the drop-down list.
     - IPv6 Network: In the Add IPv6 Network panel, complete the following, and then click Add to add to the network to the list:
       - Address: Enter an IPv6 network address and select the netmask from the drop-down list.
       - Permission: Select Allow or Deny from the drop-down list.
     - TSIG Key: In the Add TSIG Key panel, complete the following, and then click Add to add the TSIG key to the list:
       - Key name: Enter a meaningful name for the key, such as a zone name or the name of the remote name server with which the local server authenticates zone transfer requests and replies. This name must match the name of the same TSIG key on other name servers that use it to authenticate zone transfers with the local server.
       - Key Algorithm: Select either HMAC-MD5 or HMAC-SHA256.
       - Key Data: To use an existing TSIG key, type or paste the key in the Key Data field. Alternatively, you can select the key algorithm, select the key length from the Generate Key Data drop down list, and then click Generate Key Data to create a new key.
     - DNSOne 2.x TSIG Key: Select this when the other name server is a NIOS appliance running DNS One 2.x code. The appliance automatically populate the value of the key in the Value field. The Permission column displays Allow by default. You cannot change the default permission.
   - Any Address/Network: Select to allow or deny the local appliance to send zone transfers to any IP address. After you have added access control entries, you can do the following:
     - Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL icon and enter a name in the Convert to Named ACL dialog box. The appliance creates a new named ACL and adds it to the Named ACL panel. Note that the ACEs you configure for this operation stay intact.
     - Reorder the list of ACEs using the up and down arrows next to the table.
     - Select an ACE and click the Edit icon to modify the entry.
     - Select an ACE and click the Delete icon to delete the entry. You can select multiple ACEs for deletion.
   - Optionally, select the Add allowed IP addresses to also-notify check box to add all IPv4 and IPv6 addresses listed in the “Allow zone transfers to” table to the also-notify statement for each authoritative zone served by a Grid member. When you enable this, all external secondary servers that are not defined for the zone and are allowed zone transfers will receive notifications about zone updates, in addition to name servers assigned to the zone. Infoblox recommends that you do not configure a large number of external secondary servers in stealth mode. To ensure that these secondary servers receive notifications about zone updates, add their addresses to the “Allow zone transfers to” table and grant them the “Allow” permission, and then select this check box.

   Note: The appliance includes only IPv4 and IPv6 addresses. It does not include network addresses, TSIG keys, and denied addresses. When you configure a named ACL, all allowed IPv4 and IPv6 addresses in the named ACL are added to the also-notify statement.

4. Optionally, select the Add allowed IP addresses to also-notify check box to add all IPv4 and IPv6 addresses listed in the “Allow zone transfers to” table to the also-notify statement for each authoritative zone served by a Grid member. When you enable this, all external secondary servers that are not defined for the zone and are allowed zone transfers will receive notifications about zone updates, in addition to name servers assigned to the zone. Infoblox recommends that you do not configure a large number of external secondary servers in stealth mode. To ensure that these secondary servers receive notifications about zone updates, add their addresses to the “Allow zone transfers to” table and grant them the “Allow” permission, and then select this check box.

5. Optionally, you can:
   - Modify an item on the list by selecting it and clicking the Edit icon.
   - Remove an item from the list by selecting it and clicking the Delete icon.
   - Move an item up or down the list. Select it and drag it to its new position, or click the up or down arrow.
6. Save the configuration and click Restart if it appears at the top of the screen.

Specifying a Zone Transfer Format

The zone transfer format determines the BIND format for a zone transfer. This provides tracking capabilities for single or multiple transfers and their associated servers.

To specify a zone transfer format:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. Member: From the Data Management tab, select the DNS tab, click the Members tab -> member check box -> Edit icon. To override an inherited property, click Override next to it and complete the appropriate fields.
2. In the editor, click Toggle Advanced Mode.
3. When the additional tabs appear, click the Advanced subtab of the Zone Transfers tab to specify the zone transfer format. Select one of the following options from the Default Zone Transfer Format drop-down menu:
   - many-answers (Secondaries run BIND 8/9): includes as many records as the packet size allows
To specify root name servers for a Grid, member, or DNS view:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. Independent appliance
2. Member: From the System tab, select the System Manager tab, expand the Toolbar and click System Properties -> Edit.
3. DNS View: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit.
4. You can change the zone transfer settings as follows:
   - Maximum concurrent zone transfers: The maximum number of zone transfers that can be performed concurrently. Click Override to override the value inherited from the Grid and enter the required value. The default value is 10. Make sure that you specify a value from 1 to 100. Otherwise, the appliance displays an error message. To retain the same value as the Grid, click Inherit.
   - Maximum concurrent inbound zone transfers per remote name server: The maximum number of zone transfers that can be performed concurrently from a given remote name server. This configuration can be done on a per server basis. Click Override to override the value inherited from the Grid and enter the required value. The default value is 2. Make sure that you specify a value from 2 to 100. Otherwise, the appliance displays an error message. To retain the same value as the Grid, click Inherit.
   - Maximum concurrent SOA queries: The maximum number of concurrent queries a secondary name server sends to the primary server to find out if the zone serial numbers have been changed. Click Override to override the value inherited from the Grid and enter the required value. The default value is 20. Make sure that you specify a value from 20 to 1000. Otherwise, the appliance displays an error message. To retain the same value as the Grid, click Inherit.
5. Save the configuration and click Restart if it appears at the top of the screen.

About Root Name Servers

Root name servers contain the root zone file which lists the names and IP addresses of the authoritative name servers for each top-level domain. When a root name server receives a query for a domain name, it provides at least the names and addresses of the name servers that are authoritative for the top-level zone of the domain name.

You can configure the NIOS appliance to use Internet root name servers or custom root name servers. If you enable recursive queries and the appliance receives a recursive query it cannot resolve locally, it queries specified forwarders (if any) and then queries any root name servers you configure. If you do not specify internal root name servers and the appliance can access the Internet, it queries the Internet root name servers.

You can specify root name servers for the Grid, individual members, and user-defined DNS views. You can specify root name servers for all DNS views except the default view. The default view uses either the member level root name servers (if specified) or the Grid level root name servers.

Every Grid member has a default view. If you want to specify root name servers for a default view, override the Grid root name server setting at the member level and the default view can use the member-level setting.

Specifying Root Name Servers

To specify root name servers for a Grid, member, or DNS view:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. Member: From the Data Management tab, select the DNS tab, click the Members tab -> member check box -> Edit icon.
3. DNS View: From the Data Management tab, select the DNS tab, click the Zones tab -> dns_view check box -> Edit icon.
   - To override an inherited property, click Override next to it and complete the appropriate fields.
4. In the Grid DNS Properties and Member DNS Properties editors, you must click Toggle Advanced Mode.
5. When the additional tabs appear, click Root Name Servers.
6. Select one of the following options:
   - Use Internet root name servers: This option is selected by default.
   - Use custom root name servers: Click the Add icon and enter the following information when a new row appears:
     - Name: Enter a name for the root name server.
• **Address**: Enter the IP address of the root name server. The feature supports IPv4 or IPv6 values.

5. Optionally, you can:
   • Select a server from the list and click the Edit icon, to modify its information.
   • Select a server from the list and click the Delete icon.

6. Save the configuration and click **Restart** if it appears at the top of the screen.

### About Sort Lists

A sort list prioritizes A and AAAA records on certain networks when those records are included in responses, sorting them to the beginning of the list in the response. For example, you can define a sort list when a server has two interfaces and you want the DNS clients to prefer one interface because it has a faster link.

When you define a sort list on the NIOS appliance, you specify the following:

- The IP address or network of the source of the query
- The IP addresses or networks that the appliance lists first in its response when it receives a query from the corresponding source address

When the NIOS appliance receives a query from the specified IP address or network and the DNS lookup produces a response with multiple addresses, the NIOS appliance sorts the addresses so that those in the sort list are at the beginning of its response. This feature is also supported for the Infoblox-4030 appliance. For more information, refer to the *Infoblox DNS Cache Acceleration Application Guide*.

### Defining a Sort List

To define a sort list for a Grid, member, or DNS view:

1. **Grid**: From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Grid DNS Properties**.
   - **Member**: From the **Data Management** tab, select the **DNS** tab > **Members** tab -> **member** check box -> **Edit** icon.
   - **DNS View**: From the **Data Management** tab, click the **DNS** tab -> **Zones** tab> **dns_view** check box -> **Edit** icon.
   - To override an inherited property, click **Override** next to it and complete the appropriate fields.

2. In the editor, click **Toggle Advanced Mode**.

3. When the additional tabs appear, click **Sort List**.

4. Click the Add icon and select either **Any** to define a sort list for any address and network, or **Address/Network** to define a sort list for a particular source IP address or network.

5. Do the following in the new row:
   - If you selected **Address/Network**, enter the IP address or network of the source of the query. The feature supports IPv4 or IPv6 values.
   - Click the Add icon beside the source IP address to add the preferred IP addresses or networks for the source. You can add as many IP addresses as necessary. When you add multiple IP addresses, you can change the order of the IP addresses. Select an IP address and drag it to its new position, or click the up or down arrow, as shown in **Figure 17.2**.

**Figure 17.2** Sort List
Configuring a DNS Blackhole List

The DNS blackhole feature provides the ability to specify IP and network addresses of network devices that you do not want to use in the DNS resolution process. The DNS blackhole feature is disabled by default. When enabled, the NIOS appliance does not accept queries from IP addresses in the blackhole list and does not use them to resolve queries. For example, you can add the IP addresses of name servers that are using DNS incorrectly to prevent the NIOS appliance from accepting their queries and from using them as resolvers. You can also use this feature to fix temporary network issues. For example, you can add the IP addresses of delegated servers, configured forwarders, and DHCP servers that have temporary DNS-related issues.

You can create a DNS blackhole list for the entire Grid or create a separate list for each Grid member. For example, if one of your Grid members is behind a firewall, you might need to configure a different DNS blackhole list for this member because the clients that can access it might be mapped differently.

The appliance accepts queries from addresses and networks that are excluded from the blackhole list and uses these addresses and networks as resolvers. To add an IP address to the blackhole list, enter it and set its permission to Exclude. You can also add an IP address to the blackhole list and set its permission to Include so it’s not in the blackhole list, effectively allowing the NIOS appliance to respond to queries from that address and to use it as a resolver.

When you add a network to a DNS blackhole list, all the IP addresses in the network are not used in the DNS resolution process. If you want to allow some IP addresses within the network, add these addresses to the list and set their permission to “Exclude.” Ensure that you list these IP addresses before the network address because the appliance applies permissions to the addresses in the order they are listed. For example, when you add the network 10.10.0.0/24 to a DNS blackhole list, all 256 IP addresses in the network are put on the blackhole list. To allow DNS traffic to the IP addresses 10.10.0.55 and 10.10.0.88, add these two addresses before the network address in the DNS blackhole list, and then set their permissions to Exclude.

You can define ACEs or a named ACL to determine the IPv4 and IPv6 addresses and networks that you want to include in or exclude from a blackhole list.

Defining a DNS Blackhole List

To enable the DNS blackhole feature and configure a DNS blackhole list for a Grid or member:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   
   **Member:** From the Data Management tab, select the DNS tab, click the Members tab -> member check box -> Edit icon.
   
   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the editor, click the Blackhole tab and complete the following:

   3. Select one of the following:

      - **None:** Select this if you do not want to configure a blackhole list. The appliance allows all clients to resolve DNS queries. This is...
selected by default.

- **Named ACL**: Select this and click **Select Named ACL** to select a named ACL. Grid Manager displays the **Named ACLs** Selectors. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this, the appliance uses clients that have the **Exclude** permission in the DNS resolution process. You can click **Clear** to remove the selected named ACL.

- **Set of ACEs**: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows.
  - **IPv4 Address** and **IPv6 Address**: Select this to add an IPv4 address or IPv6 address. Click the **Value** field and enter the IP address of the client. The **Permission** column displays **Include** by default. You can change it to **Exclude** by clicking the field and selecting **Exclude** from the drop-down list. When you select **Include**, the appliance adds the IP address to the blackhole list and does not allow DNS queries and DNS resolution for this address. When you select **Exclude**, the appliance excludes the address from the blackhole list and allows DNS queries and resolution for the address.
  - **IPv4 Network**: In the **Add IPv4 Network** panel, complete the following, and then click **Add** to add the network to the list:
    - **Address**: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
    - **Permission**: Select **Allow** or **Deny** from the drop-down list.
  - **IPv6 Network**: In the **Add IPv6 Network** panel, complete the following, and then click **Add** to add the network to the list:
    - **Address**: Enter an IPv6 network address and select the netmask from the drop-down list.
    - **Permission**: Select **Allow** or **Deny** from the drop-down list.
  - **Any Address/Network**: Select to include or exclude any IP addresses and networks for the DNS resolution process. After you have added access control entries, you can do the following:
    - Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL **icon** and enter a name in the **Convert to Named ACL** dialog box. The appliance creates a new named ACL and adds it to the **Named ACL** panel. Note that the ACEs you configure for this operation stay intact.
    - Reorder the list of ACEs using the up and down arrows next to the table.
    - Select an ACE and click the Edit icon to modify the entry.
    - Select an ACE and click the Delete icon to delete the entry. You can select multiple ACEs for deletion.

4. **Save the configuration**.

### Specifying Hostname Policies

You can enforce a naming policy for the hostnames of A, AAAA, Host, MX, NS, and bulk host records based on user-defined or default patterns. For MX and NS records, the hostname restrictions apply to the text in the RDATA field (right-hand side) of the resource record name.

Records that you created before you enabled the hostname checking policy need not comply with the hostname restriction that you specify. You can select one of three preconfigured policies or define your own hostname policy with a POSIX regular expression. The policies Infoblox provides implement standard host naming restrictions according to RFC 952, DOD Internet Host Table Specification, and RFC 1123, Requirements for Internet Hosts -- Application and Support.

**Note**: The hostname restriction limits the hostname of A, AAAA, Host, MX, NS, and bulk host records only.

You can define your own hostname restriction policy at the Grid level only. At the member and zone levels, you can select a predefined policy or a policy that was defined at the Grid level. The appliance supports IDNs for DNS zones and resource records. For more information about IDNs, see **Support for Internationalized Domain Names**. You can use UTF-8 characters when you configure your own hostname checking policy.

### Defining Grid Hostname Policies

You can define new hostname policies and set the hostname policy for all zones in the Grid as follows:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Grid DNS Properties**.
2. In the **Grid DNS Properties** editor, click **Toggle Advanced Mode**.
3. When the additional tabs appear, click Host Naming.

The Host Name Policies section lists the following preconfigured record policies:

- **Strict Hostname Checking**: You can only use hostnames that contain alphanumeric characters, dashes (-), and asterisks (*). You cannot use other special characters, such as underscore (_). Note that when you select this policy, the appliance automatically applies the policy to dynamic DNS updates and zone transfers it receives. When you select this, you can enter host names through Grid Manager using punycode, but not IDNs. The appliance stores IDNs that are created through DNS updates and DNS transfers in punycode. You can monitor non-compliant host names using the Hostname Compliance report. For more information, see **Obtaining a List of Invalid Record Names**.

- **Allow Underscore**: You can only use hostnames with alphanumeric characters, dashes, and underscores ("_" and "_"). This is the default.

- **Allow Any**: You can use any hostname.

Select Default from the drop-down list in the Default column to change the Grid default hostname policy.

4. Click **Add** to define your own hostname checking policy.
5. Enter a record policy name and a regular expression string, and click **OK**. See **Appendix D, "Regular Expressions"**, for definitions of regular expressions. Note that Grid Manager does not validate the regular expressions that you enter. Therefore, you can inadvertently specify an invalid regular expression that might cause noncompliance errors when you create records.
6. If you select the Strict Hostname Checking policy, the **Apply policy to dynamic updates and inbound zone transfers (requires Strict Hostname Checking setting)** option is enabled by default. It enables the appliance to apply the policy to dynamic DNS updates and zone transfers that it receives. You can then select which action the appliance takes when it encounters names that do not conform to the policy. Select either **Fail** or **Warn**. If you select **Warn**, the appliance allows the dynamic DNS update or zone transfer, but logs a syslog message.

   **Note:** The Strict Hostname Checking policy only allows alphanumeric characters and dashes ("-”). In addition, this policy allows IDNs that are written in punycode. You cannot use other special characters, such as underscore ("_”). Therefore, DDNS updates from Microsoft Active Directory controllers may not be accepted.

7. Save the configuration and click **Restart** if it appears at the top of the screen.

---

### Defining Hostname Restrictions

You can select a hostname restriction policy for an individual Grid member or zone. You can specify hostname restrictions for authoritative forward-mapping zones only. You cannot specify hostname restrictions for forward zones, stub zones, IPv4 reverse-mapping zones, and IPv6 reverse mapping zones.

To select a hostname restriction policy for a Grid member or zone:

1. **Member:** From the **Data Management** tab, select the **DNS** tab, click the **Members** tab -> **member** check box -> **Edit** icon.
   **Zone:** From the **Data Management** tab, select the **DNS** tab and click the **Zones** tab -> **dns_view** -> **zone** check box -> **Edit** icon.
   
   To override an inherited property, click **Override** next to it and complete the appropriate fields.

2. In the **Member DNS Properties editor**, click **Toggle Advanced Mode**.
3. When the additional tabs appear, click **Host Naming**.
4. Click **Override**.
5. From the **Host Name Policy** drop-down list, select a predefined policy or a policy that was defined at the Grid level.
6. If you select the Strict Hostname Checking policy, the **Apply policy to dynamic updates and inbound zone transfers (requires Strict Hostname Checking setting)** is enabled by default. It enables the appliance to apply the policy to dynamic DNS updates and zone transfers that it receives. You can then select which action the appliance takes when it encounters names that do not conform to the policy. Select either **Fail** or **Warn**. If you select **Warn**, the appliance allows the dynamic DNS update or zone transfer, but logs a syslog message.

   **Note:** The strict hostname checking policy only allows alphanumeric characters and dashes. It does not allow for the use of other special characters, such as underscore ("_”). Therefore, DDNS updates from Microsoft Active Directory controllers might not be accepted.

7. Save the configuration and click **Restart** if it appears at the top of the screen.

---

### Obtaining a List of Invalid Record Names

You can retrieve a list of all record names that do not comply with the current hostname checking policy of a zone. These could be records that were created before the current host naming policy was set. In addition, if you selected the Strict Hostname Checking policy and allowed illegal hostnames in DDNS updates and inbound zone transfers with a warning, those records are listed in this report as well.

To display the Hostname Compliance report:

1. From the **Data Management** tab, select the **DNS** tab and click the **Zones** tab -> **dns_view** -> **zone** check box.
2. Click **Hostname Compliance**.
   
   The Hostname Compliance Report for the zone displays. It lists the record name, type, value, and comment for all records that do not comply with the hostname restriction policy of the zone.

From the report, you can select a record and do the following:

- Click the **Edit** icon to open the record editor.
- Click the **Delete** icon to move it to the Recycle Bin.

### About DNS64

To support the increasing number of IPv6 and dual-stack networks, Infoblox DNS servers now support DNS64, a mechanism that synthesizes AAAA records from A records when no AAAA records exist. When you enable DNS64 on an Infoblox DNS server, it can operate with a third-party NAT64 device so IPv6-only nodes can communicate with IPv4-only nodes without any changes to either of the devices.

As illustrated in **Figure 17.3**, when an IPv6-only host requests the AAAA record of an IPv4-only server and none exists, a DNS64-enabled server can retrieve the A record of the IPv4 server and synthesize an AAAA record. The IPv6-only host can then use the synthesized AAAA record, which contains the IPv6 proxy address for the IPv4 address in the original A record, to initiate communication with the IPv4 host.

**Figure 17.3**
Following are the steps illustrated in Figure 17.3:

1. An IPv6-only host sends a recursive query for the AAAA record of the IPv4 server mail1.corpxyz.com.
2. The Infoblox DNS server attempts to resolve the request for the AAAA record, and determines that an AAAA record for mail1.corpxyz.com does not exist. The DNS server then performs a query for the A record of mail1.corpxyz.com.
3. The DNS server creates a synthetic AAAA resource record from the information in the A record, and returns the synthesized AAAA record to the requesting IPv6 host.
4. The host receives the synthetic AAAA record and sends a packet to the destination address specified in the synthetic AAAA record. The packet is routed to the IPv6 interface of the NAT64 device, which translates the packet from IPv6 to IPv4 and forwards it to the server, mail1.corpxyz.com.

Infoblox DNS servers can return synthesized AAAA records to both IPv4 and IPv6 clients when the client explicitly requests an AAAA record and none exists for the requested host. If a host has multiple A records, the DNS server synthesizes an AAAA record for each A record. Infoblox DNS servers can also synthesize records for reverse-mapping zones. When a DNS server receives a query for a PTR record in the IP6.ARPA domain whose address matches a configured DNS64 prefix, the server synthesizes a CNAME record that contains an IPv4 address derived from the IPv6 address in the query. The server then sends a query for the PTR record so it can resolve the IPv4 address to the hostname. For example, if a DNS server that is configured to synthesize records for the prefix 2001:db8::/96 receives a query for the PTR record of 2001:db8::0102:0304, it synthesizes a CNAME record that contains the IPv4 address 4.3.2.1.in-addr.arpa. The server then resolves the PTR record of the IPv4 address 4.3.2.1.in-addr.arpa.

If the server obtains the PTR record, then it sends the synthesized CNAME record and the PTR record to the client. If the zone exists, but there is no PTR record, then the server sends the synthesized CNAME record only. If the zone does not exist, then the server responds with a SERVFAIL with no answers.

Additionally, Infoblox DNS servers can generate synthesized records for DNSSEC secure zones, but only for non-DNSSEC clients. A DNS client or resolver includes the EDNS OPT pseudo-RR with the DO (DNSSEC OK) bit set to indicate that they are requesting DNSSEC data. DNS servers can generate synthesized AAAA records only when the request does not have the DO bit set. This ensures that DNSSEC clients receive only valid responses.

For additional information about DNS64, refer to the following Internet drafts:


Configuring DNS64

You can enable DNS64 on both authoritative and recursive DNS servers. You can configure DNS64 at the Grid, member or DNS view level.

To configure DNS64 on Infoblox DNS servers:

1. Create at least one DNS64 synthesis group. A synthesis group specifies the IPv6 prefix of the synthesized AAAA records. For more information, see Adding a DNS64 Synthesis Group.
2. Optionally, specify additional parameters for the synthesis group. For more information, see Setting DNS64 Group Properties.
3. Enable the DNS64 service and assign a synthesis group to the Grid, a member or a DNS view. For more information, see Enabling DNS64 Service.

On the NAT64 device, you must specify the IPv6 prefixes that are configured on the DNS server.

About Synthesis Groups
A synthesis group specifies, among other things, the IPv6 prefix for the synthesized AAAA records. Infoblox DNS servers provide a default DNS64 synthesis group with the well-known prefix 64:FF9B::/96, which is reserved for representing IPv4 addresses in the IPv6 address space. You can keep the default group, change the prefix or delete the group. You can also add a synthesis group for a Network-Specific Prefix (NSP), which is an IPv6 prefix assigned to an organization to create IPv6 representations of IPv4 addresses.

After you create a synthesis group, you can define rules to restrict the synthesis of AAAA records to certain IPv4 addresses and networks, and specify the DNS clients and networks to which the server can send synthesized AAAA records. For more information, see Setting DNS64 Group Properties.

Note that though you can control the synthesis of AAAA records, the DNS server always synthesizes CNAME records when it receives a query for an IPv6 PTR record whose address matches a prefix in a DNS64 synthesis group. You can also configure the DNS server to generate synthesized AAAA records for DNS queries that have the DO bit set.

### Adding a DNS64 Synthesis Group

To add a synthesis group:

1. From the Data Management tab, select the DNS tab -> DNS64 Groups tab, and then click the Add icon.
2. In the DNS64 Synthesis Group wizard, complete the following:
   - **Name**: Enter a name for the group.
   - **Prefix**: The IPv6 prefix used for the synthesized AAAA records. The default is the well-known prefix 64:FF9B::/96. The prefix length must be /32, /40, /48, /56, /64, and /96, and all bits beyond the specified length must be zero.
   - **Comment**: Optionally, enter additional information about the group.
   - **Disabled**: Select this check box if you would like to disable the group at this time. Note that you cannot disable the group if it is the only group that is used by a Grid, member or DNS view that has DNS64 enabled.
   - **Apply to queries requesting DNSSEC records**: Select this to generate synthesized AAAA records for DNS64 synthesis groups that request DNSSEC data.
3. Click Next to define extensible attributes for the synthesis group. For information, see Using Extensible Attributes.
4. Save the configuration

### Viewing DNS64 Synthesis Groups

To view synthesis groups, from the Data Management tab, select the DNS tab -> DNS64 Groups tab. This tab displays the following information about each group:

- **Name**: The group name.
- **Prefix**: The IPv6 prefix that is assigned to the group.
- **Comment**: The comment that was entered for the group.
- **Site**: The value of this attribute, if specified.

You can display the following additional column:

- **Disabled**: Indicates whether the group is disabled.

You can do the following:

- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
- Edit the properties of a synthesis group.
  - Select the synthesis group, and then click the Edit icon.
  - Move a synthesis group to the Recycle Bin.
  - Select the synthesis group, and then click the Delete icon. Note that you cannot delete a synthesis group that is assigned to a Grid, member or DNS view.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Export the synthesis groups to a .csv file.
  - Click the Export icon.
- Print the list of synthesis groups.
  - Click the Print icon.

### Setting DNS64 Group Properties

After you create a DNS64 synthesis group, you can specify the following:

- The IPv4 and IPv6 DNS clients and networks to which the DNS server is allowed to send synthesized AAAA records with the specified IPv6 prefix.
- The IPv4 addresses and networks for which the DNS server can synthesize AAAA records with the specified prefix.
- IPv6 addresses or prefix ranges that cannot be used by IPv6 only hosts, such as IP addresses in the ::ffff:0:0/96 network. When the DNS server retrieves an AAAA record that contains an IPv6 address that matches an excluded address, it does not return the AAAA record. Instead, it synthesizes an AAAA record from the A record.
Note that a DNS server synthesizes the AAAA record of a host that has both A and AAAA records when all the IPv6 addresses in the AAAA records match the excluded addresses. If the host has multiple AAAA records and some of them contain excluded IPv6 addresses, then the server returns the remaining AAAA records.

You can add individual access control entries (ACEs) or use a named access control list (ACL) to define these clients. For information about how to define named ACLs, see Defining Named ACLs.

To configure DNS64 group properties:

1. From the Data Management tab, select the DNS tab -> DNS64 Groups tab -> group check box -> Edit icon.
2. In the General tab of the DNS64 Synthesis Groups editor, you can do the following:
   - Modify the name, prefix or comment.
   - Select the Disabled check box, if you want to disable the group at this time.
   - Select the Apply to queries requesting DNSSEC records check box to have the DNS server generate synthesized AAAA records for DNS64 synthesis groups that request DNSSEC data.

Perform DNS64 synthesis for these clients: Specify IPv4 and IPv6 hosts and networks to which Infoblox DNS servers can send synthesized AAAA records. The default is to allow any IPv4 and IPv6 address and network. Select one of the following:
   - **None**: Select this if you do not want to define specific addresses or networks to which the appliance sends synthesized AAAA records. When you select this, the appliance sends synthesized AAAA records to all clients. This is selected by default.
   - **Named ACL**: Select this and click Select Named ACL to select a named ACL. Grid Manager displays the Named ACLs Selecto r. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this option, the appliance sends synthesized AAAA records to the clients that have the Allow permission in the list. You can click Clear to remove the selected named ACL.
   - **Set of ACEs**: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list:
     - IPv4 Address and IPv6 Address: Select this to add an IPv4 address or IPv6 address. Click the Value field and enter the IP address. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.
     - IPv6 Network: In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
       - **Address**: Enter an IPv6 network address and either type a netmask or move the slider to the desired netmask.
       - **Permission**: Select Allow or Deny from the drop-down list.
     - IPv4 Network: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
       - **Address**: Enter an IPv4 network address and select the netmask from the drop-down list.
       - **Permission**: Select Allow or Deny from the drop-down list.
     - Any Address/Network: Select this to allow or deny any IP addresses to which the appliance sends synthesized AAAA records.

Mapped IPv4 Addresses: Specify IPv4 addresses and networks for which the DNS server synthesizes AAAA records. The default is to allow the DNS server to synthesize AAAA records for any IPv4 address in any network. Select one of the following:
   - **None**: Select this if you do not want to define specific IPv4 addresses or networks for which the DNS server synthesizes AAAA records. The appliance synthesizes AAAA records for all IPv4 clients. This is selected by default.
   - **Named ACL**: Select this and click Select Named ACL to select a named ACL. Grid Manager displays the Named ACLs Selecto r. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this option, the appliance sends synthesized AAAA records for the clients that have the Allow permission in the list. You can click Clear to remove the selected named ACL.
   - **Set of ACEs**: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list:
     - IPv4 Address and IPv6 Address: Select this to add an IPv4 address or IPv6 address. Click the Value field and enter the IP address. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.
     - IPv6 Network: In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
       - **Address**: Enter an IPv6 network address and select the netmask from the drop-down list.
       - **Permission**: Select Allow or Deny from the drop-down list.
     - IPv4 Network: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
       - **Address**: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
       - **Permission**: Select Allow or Deny from the drop-down list.
     - Any Address/Network: Select this to allow or deny any IP addresses for which the appliance sends synthesized AAAA records.

Exclude IPv6 addresses: Specify IPv6 addresses of AAAA records that the appliance treats as nonexistent. The DNS server does not return the AAAA record of an address from this list. Instead, it synthesizes an AAAA record.
   - **None**: Select this if you do not want to define specific IPv6 addresses or networks of AAAA records that the appliance treats as nonexistent. The appliance treats all IPv6 addresses as nonexistent. This is selected by default.
   - **Named ACL**: Select this and click Select Named ACL to select a named ACL. Grid Manager displays the Named ACLs Selecto r. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this option, the appliance synthesizes AAAA records from A records for the clients that have the Allow permission in the list. You can click Clear to remove the selected named ACL.
   - **Set of ACEs**: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list.
Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows.

- **IPv6 Address:** Select this to add an IPv6 address. Click the Value field and enter the IP address. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.
- **IPv6 Network:** In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
  - **Address:** Enter an IPv6 network address and select the netmask from the drop-down list.
  - **Permission:** Select Allow or Deny from the drop-down list.
- **Any Address/Network:** Select this to allow or deny any IP addresses of AAAA records that the appliance treats as nonexistent. After you have added access control entries, you can do the following:
  - Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL icon and enter a name in the Convert to Named ACL dialog box. The appliance creates a new named ACL and adds it to the Named ACL panel. Note that the ACEs you configure for this operation stay intact.
  - Reorder the list of ACEs using the up and down arrows next to the table.
  - Select an ACE and click the Edit icon to modify the entry.
  - Select an ACE and click the Delete icon to delete the entry. You can select multiple ACEs for deletion.
- **Extensible Attributes:** You can modify the attributes. For information, see Using Extensible Attributes.
- **Permissions:** This tab displays if you logged in as a superuser. For information, see About Administrative Permissions.

3. Save the configuration and click Restart if it appears at the top of the screen.

**Enabling DNS64 Service**

You can enable DNS64 at the Grid, member, and DNS view level. At least one DNS64 synthesis group must be configured before you can enable DNS64.

To enable DNS64 and apply DNS64 synthesis groups:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. **Member:** From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon. **DNS View:** From the Data Management tab, select the DNS tab -> Zones tab -> dns_view check box -> Edit icon. To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the Grid and Member DNS Properties editor, click **Toggle Advanced Mode**, and then click DNS64. In the View DNS Properties editor, just click DNS64.

3. Do the following in the DNS64 tab:

   - **Enable DNS64:** Select this check box.
   - **Synthesis Groups:** Click the Add icon and select a synthesis group.

4. Save the configuration and click Restart if it appears.

**DNS Record Scavenging**

The DNS scavenging feature allows you to remove unused DNS resource records from zone data to prevent the accumulation of unneeded records. A scavenging operation determines, based on predefined rules, which records are not needed, i.e. are reclaimable, and removes them. For information about scavenging rules, see Scavenging Rules.

Scavenging is used for records with the dynamic record source type. Dynamic records are those created automatically, for example, via a dynamic DNS update. Static records, i.e. records that you add manually, can be identified as reclaimable based on scavenging rules but are not subject to scavenging. You can see the source type for each record in the DNS Resource Records viewer in Grid Manager.

You can use the records scavenging feature at the following levels in NIOS:

- **Grid:** scavenging is performed in all views and zones of the Grid.
- **DNS view:** scavenging is performed in all zones of the view.
- **Authoritative zone (a Grid primary or unassigned zone):** scavenging is performed in the specified zone, but not in the subzones.

You can either scavenge DNS records immediately or schedule automatic scavenging. For more information, see Scavenging DNS Records Immediately and Scheduling Automatic Scavenging.

You can organize and monitor records identified as reclaimable by using Smart Folders. For information, see Chapter 3, Smart Folders. Scavenging events are logged in the NIOS syslog. You can view it, as described in Viewing the Syslog and Searching in the Syslog. The records are removed to the Recycle Bin and can be restored from there. For more information, see Restoring Reclaimed Records.

You can either scavenge DNS records immediately or schedule automatic scavenging. For more information, see Scavenging DNS Records Immediately and Scheduling Automatic Scavenging.

You can organize and monitor records identified as reclaimable by using Smart Folders. For information, see Chapter 3, Smart Folders. Scavenging events are logged in the NIOS syslog. You can view it, as described in Viewing the Syslog and Searching in the Syslog. The records are removed to the Recycle Bin and can be restored from there. For more information, see Restoring Reclaimed Records.

**Note:** Membership in the DNS Admin group is required to complete scavenging operations. For details, see Administrative Permissions for DNS Records Scavenging. Also see Forcing Creation Timestamp Initialization for Unchanged Records for information on handling the creation timestamp of records that remain unchanged at DDNS updates.

**Scavenging Rules**

You can configure the following match rules to identify reclaimable DNS resource records:

- **Resource Record Type:** This rule allows you to specify the record type to run scavenging on. A record is reclaimable if its type matches or does not match the type specified in the rule. The record types that support scavenging include the following:
  - A
  - AAAA
To configure the DNS record scavenging properties:

- **Object Properties:** The scavenging properties configured at a given level are inherited by the level below, unless overridden.

To override the inherited properties, click **Edit icon.**

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view check box -> Edit icon.
3. From the Data Management tab, select the DNS tab and click the Zones tab -> click a DNS view -> zone check box -> Edit icon.

3. If the properties editor is in basic mode, click Toggle Advanced Mode.
4. Click DNS Scavenging.
5. Enable last queried time monitoring for resource records: Select this if you are going to use the Last Queried Time rule. This setting enables monitoring the time when the resource record was last queried for its DNS data. For more information on DNS queries monitoring for resource records, see Monitoring DNS Queries.
6. Enable last queried time monitoring for zones: This setting enables monitoring the time when the zone, i.e. at least a single record in it, was last queried for its DNS data. The data resulting from zone last queries time monitoring is displayed in the zones viewer (Data Management -> DNS -> Zones -> click a DNS view to open zones list).

**Note:** Enabling monitoring for a zone does not enable monitoring for child zones.

1. Select Enable record scavenging.
2. To override the inherited properties, click Override and complete the fields.
3. Under **Match the following rule,** create a rule as follows. For information about rules, see Scavenging Rules.
   - **Choose Filter:** Select a criterion from the drop-down list.
   - **Choose Operator:** Select an operator for the filter criterion.
   - In the value field, enter the value for the filter field. To add another rule:
     - Click + to add another rule at the same level.
     - Click => to add an all (logical AND) or any (logical OR) operator line and a parenthetical rule that is indented one level above the first rule.
     - Click <= to add an all (logical AND) or any (logical OR) operator line and a parenthetical rule that is indented one level above the first rule.

   To logically combine the whole ruleset, select **Match all of the following rules or Match any of the following rules**.

   After you add all the match rules, you can click **Reset** to remove the previously configured rules and start again.

4. Under **Match records with the following extensible attribute,** add an extensible attribute to use as an additional criterion for finding necessary records.
   - **Choose Filter:** Select a criterion from the drop-down list.
   - **Choose Operator:** Select an operator for the filter criterion.
   - In the value field, enter the value for the filter field.

   To add another extensible attribute, click +.

   To logically combine the extensible attributes set, select **Match all records with the following extensible attributes or Match any records with the following extensible attributes**.

   After you add all the extensible attributes, you can click **Reset** to remove the previously configured attributes and start again.

**Note:** In the case of upgrade to NIOS 7.3, the creation time is not initialized. Therefore the "Creation Time" rule does not apply to the records created before the upgrade.

**Note:** If you use this rule, also select **Enable last queried time monitoring for resource records** in the Grid, view, or zone scavenging properties, as described in the next section.

**Last Discovered Time:** This rule allows you to identify reclaimable records based on the record's last discovered timestamp. This rule is applicable to A, AAAA, and PTR records.

**Record Source:** This rule allows you to specify the record source – static or dynamic – to be used as a filter when identifying reclaimable records.

**Associated Records:** This rule allows you to identify reclaimable records based on whether they have or do not have associated records. Record associations are supported for address records (A, AAAA, and PTR). Additionally, you can reclaim the associated records when reclaiming the original ones by enabling the option When reclaiming A, AAAA, or PTR records, also reclaim the corresponding, symmetric A, AAAA, and PTR records in the scavenging properties, as described in the next section.

**Extensible Attributes:** You can specify extensible attributes that reclaimable records should match in addition to the scavenging rules described above.

**Configuring DNS Record Scavenging Properties**

You can configure the DNS record scavenging properties at the Grid, DNS view, or DNS zone level. According to the NIOS inheritance pattern for object properties, the scavenging properties configured at a given level are inherited by the level below, unless overridden.

To configure the DNS record scavenging properties:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. DNS view: From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view check box -> Edit icon.
3. DNS zone: From the Data Management tab, select the DNS tab and click the Zones tab -> click a DNS view -> zone check box -> Edit icon.
4. If the properties editor is in basic mode, click Toggle Advanced Mode.
5. Click DNS Scavenging.
6. Enable last queried time monitoring for resource records: Select this if you are going to use the Last Queried Time rule. This setting enables monitoring the time when the resource record was last queried for its DNS data. For more information on DNS queries monitoring for resource records, see Monitoring DNS Queries.
7. Enable last queried time monitoring for zones: This setting enables monitoring the time when the zone, i.e. at least a single record in it, was last queried for its DNS data. The data resulting from zone last queries time monitoring is displayed in the zones viewer (Data Management -> DNS -> Zones -> click a DNS view to open zones list).

**Note:** Enabling monitoring for a zone does not enable monitoring for child zones.

8. Select Enable record scavenging.
9. To override the inherited properties, click Override and complete the fields.
10. Under **Match the following rule,** create a rule as follows. For information about rules, see Scavenging Rules.
    - **Choose Filter:** Select a criterion from the drop-down list.
    - **Choose Operator:** Select an operator for the filter criterion.
    - In the value field, enter the value for the filter field. To add another rule:
      - Click + to add another rule at the same level.
      - Click <= to add an all (logical AND) or any (logical OR) operator line and a parenthetical rule that is indented one level above the first rule.

    To logically combine the whole ruleset, select **Match all of the following rules or Match any of the following rules**.

    After you add all the match rules, you can click **Reset** to remove the previously configured rules and start again.

11. Under **Match records with the following extensible attribute,** add an extensible attribute to use as an additional criterion for finding necessary records.
    - **Choose Filter:** Select a criterion from the drop-down list.
    - **Choose Operator:** Select an operator for the filter criterion.
    - In the value field, enter the value for the filter field.

    To add another extensible attribute, click +.

    To logically combine the extensible attributes set, select **Match all records with the following extensible attributes or Match any records with the following extensible attributes**.

    After you add all the extensible attributes, you can click **Reset** to remove the previously configured attributes and start again.
11. **When reclaiming A, AAAA or PTR records, also reclaim the corresponding, symmetric A, AAAA and PTR records**: Select this if you want to reclaim records associated to the ones identified as reclaimable.

12. **To configure a schedule for automatic records scavenging**, select **Enable scheduled record scavenging**. See [Scheduling Automatic Scavenging](#). 

13. **Click Save & Close** or **Save**.

### Scheduling Automatic Scavenging

You can schedule a scavenging operation only at the Grid level. For a scavenging operation at the view or zone level, you can use the schedule inherited from the Grid.

**Note:** Infoblox recommends manually testing the configured scavenging settings before enabling scheduled scavenging.

1. In the DNS record scavenging properties described in the previous section, select the **Enable scheduled record scavenging** check box.
2. To enable automatic scavenging after records are marked as reclaimable, select **After marking a record as reclaimable, automatically reclaim the record**.
3. Click the **Scheduling** icon and complete the following in the Scavenging Scheduler dialog:
   - Select how often you want to execute the scavenging. You can select **Once**, **Hourly**, **Daily**, **Weekly**, or **Monthly**.
     - **If you select Once**, complete the following:
       - Enter the day in the date picker and select a month from the drop-down list.
       - Enter a time in the hh:mm:ss AM/PM format. You can also select a time from the drop-down list.
       - Choose the **Time Zone**.
     - **If you select Hourly**, complete the following:
       - **Schedule every hour(s) at**: Enter the number of hours between each scavenging instance. You can enter a value from 1 to 24.
       - **Minutes past the hour**: Enter the number of minutes past the hour. For example, enter 5 if you want to schedule the scavenging operation five minutes after the hour.
       - Choose the **Time Zone**.
     - **If you select Daily**, complete the following:
       - Click either **Every day** or **Every weekday**.
       - Enter a time in the hh:mm:ss AM/PM format. You can also select a time from the drop-down list.
       - Choose the **Time Zone**.
     - **If you select Weekly**, complete the following:
       - **Schedule every week on**: Select any day of the week.
       - Enter a time in the hh:mm:ss AM/PM format. You can also select a time from the drop-down list.
       - Choose the **Time Zone**.
     - **If you select Monthly**, complete the following:
       - **Schedule the day of the month**: Enter the day of the month and the monthly interval. For example, to schedule the rule update on the first day after every 2 months, you can enter Day 1 every 2 month(s).
       - Enter a time in the hh:mm:ss AM/PM format. You can also select a time from the drop-down list.
       - Choose the **Time Zone**.
   - **Click OK**.

### Scavenging DNS Records Immediately

To perform record scavenging for the Grid, a DNS view, or a zone according to the predefined rules, use the Scavenge Records command from the Toolbar. This adds a background task that starts immediately or, if another scavenging task is in progress, after its completion. The scavenging is split into two stages that you can execute separately or together:

- **Mark records as reclaimable**: This stage analyzes the records against the scavenging rules. The records matching the rules are marked as reclaimable, i.e. their "Reclaimable" flag is set to "Yes" in the DNS Resource Records viewer. These records can be reclaimed by using the second stage, unless you disable scavenging for them as described in [Disabling Scavenging for Individual Records](#).
- **Reclaim records marked as reclaimable**: This stage automatically removes the records marked as reclaimable in the result of the execution of the first option. Running only the "Reclaim records marked as reclaimable" stage without the analysis stage does not perform a new analysis on the affected records. It only removes the records marked as reclaimable during the previous analysis.

Also, you can reset the reclaimable flag of the records. As an example of when this may be useful: if records have previously been marked as reclaimable and under a revised scavenging policy some records may no longer be reclaimable.

**Note:** To start immediate scavenging of DNS records, you must first carefully define the scavenging properties, as described in [Configuring DNS Record Scavenging Properties](#).

To scavenge DNS records immediately:
1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Scavenge Records ➝ Scavenge Grid Records.

   DNS view: From the Data Management tab, select the DNS tab, click a DNS view, expand the Toolbar, and then click Scavenge Records ➝ Scavenge View Records.

   DNS zone: From the Data Management tab, select the DNS tab, click a DNS view, click a zone, expand the Toolbar, and then click Scavenge Records ➝ Scavenge Zone Records.

2. Select one of the following:
   - **Scavenge Records**: Select this to proceed to the record scavenging. Go to the next step.
   - **Reset reclaimable flag**: Select this to set the "Reclaimable" flag of all affected records to "No".
   - **Mark records are reclaimable**
   - **Reclaim records marked as reclaimable**

   **Note**: Static records are never reclaimed automatically even if they are marked as reclaimable. You can only delete static records manually from the DNS Resource Records viewer.

3. If you chose Scavenge Records, select one of the following options or both of them:
   - **Scavenge Records**
   - **Mark records are reclaimable**
   - **Reclaim records marked as reclaimable**

   **Note**: Keep in mind that the Enable record scavenging property for a lower scavenging scope (e.g. view or zone) can override this property for the upper scope (i.e., Grid or view respectively). For example, if you run scavenging on the Grid with the scavenging option disabled, and there are some views or zones on which scavenging is enabled, this results in the records of the affected views and zones being scavenged. Vice versa, if scavenging is disabled for certain views or zones and you run scavenging on the Grid with the scavenging option enabled, the corresponding views and zones are excluded from scavenging.

4. Click **Start**.

   To check the progress of the current scavenging task, you can use the DNS Record Scavenging widget in the Dashboard. For more information, see DNS Record Scavenging. You can also view a scavenging report, as described in DNS Scavenged Object Count Trend. The scavenging task may be subject for an approval workflow. For information on approval workflows, see Configuring Approval Workflows.

**Note**: Keep in mind that the Enable record scavenging property for a lower scavenging scope (e.g. view or zone) can override this property for the upper scope (i.e., Grid or view respectively). For example, if you run scavenging on the Grid with the scavenging option disabled, and there are some views or zones on which scavenging is enabled, this results in the records of the affected views and zones being scavenged. Vice versa, if scavenging is disabled for certain views or zones and you run scavenging on the Grid with the scavenging option enabled, the corresponding views and zones are excluded from scavenging.

### Disabling Scavenging for Individual Records

You can disable scavenging for individual records, even if they are marked as reclaimable. In this case, the record is never reclaimed unless you enable the scavenging for it again.

To disable scavenging for a record:

1. In the DNS Resource Records viewer, select the appropriate record.
2. Click **Edit**.
3. In the record properties dialog, click DNS Scavenging.
4. Select the **Disable scavenging for this record** check box.
5. Click **Save & Close**.

   Additionally, you can see the following information in the resource record scavenging properties:

   - Record creation time
   - Record last queried time
   - Whether the record is reclaimable

   For records synced from MS servers, the creation timestamp is not synced. This implies the following limitations:

   - When a zone is converted from MS to NIOS, the timestamp is initialized to the time when the operation occurs.
   - When a zone is converted from NIOS to MS, the timestamp is reset.

### Administrative Permissions for DNS Records Scavenging

By default, only superusers can perform DNS records scavenging. Limited-access users can use the scavenging functionality if they have the corresponding DNS scavenging permissions. For more information about admin permissions, see About Administrative Permissions. The DNS scavenging permissions are global to Grid Manager. They are used in addition to the regular DNS global and object permissions. For more information about the DNS permissions, see Administrative Permissions for DNS Resources.

The following operations require scavenging permissions:

- Modifying scavenging properties for the Grid, a view, or a zone
- Configuring a scavenging schedule
- Performing a scavenging task
- Viewing the DNS Record Scavenging dashboard widget
- Viewing the DNS Scavenged Object Count Trend report

### Restoring Reclaimed Records

A reclaimed record remains in the Recycle Bin until the bin is emptied. You can restore the deleted records from the Recycle Bin, as described in Restoring Objects from the Recycle Bin.
The Recycle Bin does not display information on whether a record was deleted during a scavenging process or manually. Therefore, you cannot restore the reclaimed data only.

When a record is restored from the Recycle Bin, its Reclaimable flag is reset to "No".

**Note:** Only a super user can restore records reclaimed during a recurring scavenging task.

**Monitoring DNS Queries**

You can monitor DNS resource records by their Last Queried time. You can configure this feature in the Grid DNS Properties editor -> DNS Scavenging tab. Infoblox recommends that you keep the number of zones or domains for monitoring below 1000; specifying more may adversely affect performance.

To view DNS queries by their Last Queried time:

1. From the Data Management tab -> DNS tab, click the Query Monitoring tab.
2. The Query Monitoring tab provides a Last Queried report for the monitored resource records, including the following information:
   - **Network View:** Network view name. You cannot sort on this column. This column is hidden by default.
   - **DNS View:** DNS view name. This column is hidden by default. **Zone:** FQDN of zone.
   - **Name:** FQDN of resource record.
   - **Record Type:** Resource record type.
   - **Record Data:** Value of resource record, such as address of an A record.
   - **Monitored Since:** Date monitoring started.
   - **Last Queried:** Displays "Not Monitored", "Not Queried Since xxxx", or date of last query.

**Note:** This report does not display the last queried information for automatically generated NS records.

To enable last queried time monitoring for resource records, do the following in the DNS scavenging properties for the Grid, a view, or a zone:

1. **Grid:** From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   
   DNS view: From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view check box -> Edit icon.
   
   DNS zone: From the Data Management tab, select the DNS tab and click the Zones tab -> click a DNS view -> check box -> Edit icon.
2. If the properties editor is in basic mode, click **Toggle Advanced Mode**.
3. Click DNS Scavenging.
4. Select the Enable last queried time monitoring for resource records check box. For more information, see Configuring DNS Record Scavenging Properties.
5. Click **Save & Close**.

**Note:** Exporting the query monitoring data may take longer than usual if the report contains a lot of records. Also, if a Grid secondary server uses zone transfer to update zone data from a Grid primary server, NIOS does not monitor queries made to the Grid secondary server and it does not update the last queried timestamp for the resource records in a zone.

When multiple values are specified with the same filter, the filter applies or logic, e.g. ‘a’ or ‘b’. Other perspectives in NIOS UI apply and logic, e.g., ‘a’ and ‘b’. You can use the following filters to get specific information in this report:

- **DNS View:** DNS view name.
- **Not Queried:** Specify a date when the last query was made. The only operator is "Since".
- **Zone:** FQDN of zone.
- **Type:** Only a single record type filter can be specified. This filter has the following resource records:
  - A Records
  - AAAA Records
  - BulkHost
  - CNAME Records
  - DNAME Records
  - DS Records
  - DTC LBDN Records
  - Host Address
  - Host Alias
  - Host Record
  - MX Records
  - NAPTR Records
  - NS Records
  - PTR Records
  - Resource Record
  - SRV Records
  - Shared A Record
  - Shared AAAA Record
  - Shared CNAME Record
  - Shared MX Record
  - Shared SRV Record
  - TXT Records
**Configuring DNS Traffic Control Properties**

You can configure the DNS Traffic Control properties at the Grid or member level. The member DTC properties are inherited from the Grid DTC properties unless you override them.

The following sections explain how to configure DTC properties for the Grid or a Grid member.

**Configuring Grid DNS Traffic Control Properties**

To configure DNS Traffic Control properties for the Grid:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Grid DNS Properties**.
2. In the **Traffic Control** tab, complete the following:
   - **Extensible Attributes Source Types for Topology Rules**: Specify up to four extensible attributes to use as source types when defining DNS traffic control topology rules. For information about the extensible attribute topology rules, see **Defining Topology Rules**.
     - You can use either predefined EAs or your own. For information about predefined extensible attributes, see **About Extensible Attributes**.
   - **When DNS Traffic Control is enabled, direct traffic according to EDNS0 Client Subnet when possible**: Select this check box to direct traffic according to EDNS0 client subnet option when DNS Traffic Control is processing DNS queries.
     - You can enable the appliance to redirect traffic according to EDNS0 client subnet option when DNS Traffic Control is processing DNS queries that contain the EDNS0 client subnet option when DNS Traffic Control is processing DNS queries. When you enable this feature, DNS Traffic Control querying process uses the client address specified in the EDNS0 client subnet option of the DNS query and the appliance includes the EDNS0 client subnet option in the response message. If there are multiple EDNS0 client subnet options in a query, the appliance considers only the first option and ignores the other options. When this feature is disabled, DNS Traffic Control querying process ignores the EDNS0 client subnet option. For more information about EDNS0, see **Using Extension Mechanisms for DNS (EDNS0)**.
   - **Return DNS responses if there are no DTC responses available**: Select this if you want the appliance to return DNS responses if no DNS traffic control responses are available.
   - **Return the following type of response from DNSSEC signed zones**: Select one of the following response types for DNSSEC-signed zones:
     - Signed
     - Unsigned
     - For more information on the Signed and Unsigned modes, see **Managing LBDN Records** and **Configuring Grid DNS Traffic Control Properties**.
3. Save the configuration and click **Restart** if it appears at the top of the screen.

**Configuring Member DNS Traffic Control Properties**

To configure DNS Traffic Control properties for a Grid member:

1. From the **Data Management** tab, select the **DNS** tab -> **Members** tab -> **member** check box -> **Edit** icon.
   Alternatively, you can select the **DNS** tab -> **Traffic Control** tab, click **Member DNS Properties** in the Toolbar, and then select the required member.
2. In the **Traffic Control** tab, complete the following:
   - **DTC Health Check Source**: Select which NIOS network interface to use for the DTC health check. Choose one of the following:
     - ANY
     - VIP
     - LAN2
     - MGMT
     - IP (This is displayed only when you have configured additional IP addresses in the network settings. Specify the IP address of the source.)
   - **When DNS Traffic Control is enabled, direct traffic according to EDNS0 Client Subnet when possible**: To retain the same setting as the Grid, keep the inherited value. To override the Grid setting, click **Override**. For information, see **Configuring Grid DNS Traffic Control Properties**.
3. Save the configuration and click **Restart** if it appears at the top of the screen.

**Chapter 18 DNS Views**

DNS views enable the NIOS appliance to serve different versions of DNS data based on the host accessing it. The topics in this chapter include:
Using Infoblox DNS Views

DNS views provide the ability to serve one version of DNS data to one set of clients and another version to another set of clients. With DNS views, the NIOS appliance can provide a different answer to the same DNS query, depending on the source of the query. In Figure 18.1, the appliance has two views: an Internal and an External DNS view. When the appliance receives queries from DNS clients, it responds with data from either the Internal or External DNS view, depending on the source IP address. When the appliance receives a query from Client A and determines that it can resolve the query from data in the Internal view, the appliance responds with the IP address of the site in the Internal view. When the appliance receives a query from Client B and determines that it can resolve the query from data in the External view, it responds with the IP address in the External view.

You can configure both forward and reverse mapping zones in DNS views and provide DNS services, such as name resolution, zone transfers and dynamic DNS updates. For information about these services, see Configuring DNS Services.

You can provide multiple views of a given zone with a different set of records in each DNS view. In Figure 18.2, both views contain the corpxyz.com zone and the sales.corpxyz.com zone. The finance.corpxyz.com zone is only in the internal DNS view, and only internal users are allowed to access records in that zone. Resource records can also exist in multiple zones. In the example, the A records for serv1.sales.corpxyz.com and serv2.sales.corpxyz.com are in the sales.corpxyz.com zones in both views.

<table>
<thead>
<tr>
<th>Internal DNS View</th>
<th>corpxyz.com</th>
<th>sales.corpxyz.com</th>
<th>finance.corpxyz.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>MX</td>
<td>serv1.sales.corpxyz.com</td>
<td>A</td>
<td>server.finance.corpxyz.com</td>
</tr>
<tr>
<td>NS</td>
<td>dnsoneA.corpxyz.com</td>
<td>A</td>
<td>printer.finance.corpxyz.com</td>
</tr>
<tr>
<td>A</td>
<td>host1.corpxyz.com</td>
<td>A</td>
<td>fin1.finance.corpxyz.com</td>
</tr>
<tr>
<td>A</td>
<td>host2.corpxyz.com</td>
<td>A A A</td>
<td>fin2.finance.corpxyz.com</td>
</tr>
<tr>
<td>A</td>
<td>host3.corpxyz.com</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>External DNS View</th>
<th>corpxyz.com</th>
<th>sales.corpxyz.com</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
You can control which clients access a DNS view through the use of a match list specifying IP addresses and/or TSIG (transaction signature) keys. When the NIOS appliance receives a request from a client, it tries to match the source IP address and/or TSIG key with its match list when determining which DNS view, if any, the client can access. After the appliance determines that a client can access a DNS view, it checks the zone level settings to determine if it can provide the service that the client is requesting.

For information on TSIG keys or defining zone transfer settings, see Enabling Zone Transfers. For more information on match lists, see Defining Match Clients Lists. For information on defining query settings, refer to Controlling DNS Queries.

**Figure 18.3** illustrates how the NIOS appliance resolves a query for a domain name in a zone of a DNS view. In the example, the internal DNS view is listed before the external DNS view. Therefore, when the appliance receives a query, it checks the match list of the internal DNS view first. If it does not find the source address in the match list of the internal DNS view, it checks the match list of the external DNS view. The match list of the external DNS view allows all IP addresses.

Next, the NIOS appliance checks the zone level settings to determine if it is allowed to resolve queries from the client for domain names in that zone. After the appliance determines it is allowed to respond to queries from this client, it resolves the query and sends back the response to the client.

**Figure 18.3 Query Resolution**

When you create more than one DNS view, as shown in Figure 18.3, the order of the views is important. View order determines the order in which the NIOS appliance checks the match lists. In Figure 18.3, the internal DNS view is listed before the external DNS view. If the views were reversed, no hosts would receive DNS replies from the internal DNS view because the match list of the external DNS view allows replies to clients with any IP address. For information on how to order views, see Managing the DNS Views of a Grid Member.

In a Grid, each Grid member can host its own set of views. A Grid member can serve as the primary or secondary server for multiple views of a particular zone. For information about specifying primary and secondary servers, see Assigning Zone Authority to Name Servers.

### About DNS Views and Network Views

The NIOS appliance provides one default DNS view, which is always associated with the default network view. You can create additional network and DNS views. A network view is a single routing domain with its own networks. For information about network views, see Configuring DHCP for IPv4.

The default DNS view initially allows all IP addresses access, and has the same recursion setting as the Grid. You can change these properties and rename the default DNS view, but you cannot delete it. When you upgrade or migrate from a name server, or an earlier version of software that does not support DNS views, the appliance places all the zones defined in the older release in the default DNS view. You can then create additional views and organize the zones in each view.

When you create a network view, the appliance automatically creates a corresponding DNS view with “default.” prepended to the name of the network view. You can rename the system-defined DNS view and configure its properties.

If the appliance contains only one network view, all DNS views are associated with that network view. If there are 20 or less network views configured, the appliance displays the network views in the drop-down list on the left of the top navigation bar of the Data Management tab of
Grid Manager. The appliance displays the Network View Selector dialog box if there are more than 20 network views configured. You can adjust the page size of the selector by choosing the number of network views to be displayed on each page from the Page Size drop-down list. If the number of network views exceeds the selected number, the selector displays the data on multiple pages. If you have a large number of network views, select a larger page size so you can quickly locate a network view without excessive paging through the list. The default page size is 10.

A DNS view can be in one network view only, but a network view can have multiple DNS views. If you enable dynamic DNS updates, you must specify which DNS view receives the updates. In a network view, only one DNS view can receive the dynamic DNS updates. For information, see Sending DDNS Updates to a DNS Server.

Configuring DNS Views

Following are the tasks to configure a DNS view:

1. Add a DNS view, as described in Adding a DNS View.
2. Add zones to the DNS view. You can add authoritative forward-mapping and reverse-mapping zones, as well as delegated, forward, and stub zones. For information about configuring each type of zone, see Configuring Authoritative Zones and Configuring Delegated, Forward, and Stub Zones.

You can optionally do the following:

1. Define a Match Clients list and a Match Destination list to restrict access to the DNS view. For more information, see Defining Match Clients Lists and Defining a Match Destinations List.
2. Copy resource records from one zone to another. This is useful when different DNS views have the same zone and have multiple resource records in common. For information, see Managing DNS Views.
3. Create resource records in a group and share the group among multiple zones. For information, see About Shared Record Groups.
4. Specify which interface IP address is published in the glue A record of the DNS view. For information, see Changing the Interface IP Address.
5. Manage recursive views. For information, see Managing Recursive DNS Views.
6. Manage the order of the DNS views, as this determines the order in which the NIOS appliance checks the Match Clients list. For information, see Managing the Order of DNS Views.
7. Configure forwarders for a DNS view. For more information, see Using Forwarders.
8. Enable AAAA filtering and configure a list of IPv4 networks and addresses for allowing or denying AAAA filtering from the appliance. For information, see Controlling AAAA Records for IPv4 Clients.

Adding a DNS View

You can add up to 1000 DNS views. When you add a DNS view, specify the following:

- The network view in which you are creating the DNS view. The appliance lists the network views only when there are multiple network views. Otherwise, it automatically associates the DNS view with the default network view.
- A Match Clients list specifying the hosts allowed access to the DNS view. If you do not define a list, the appliance allows all hosts to access the DNS view. For more information, see Defining Match Clients Lists.
- Whether recursive queries are allowed. When a name server is authoritative for the zones in a DNS view, you can disable recursion since your name server should be able to respond to the queries without having to query other servers. Note that a DNS view actually inherits its recursion setting from the Grid members that serve its zones. When you first create a DNS view though, it does not have any zones and therefore inherits its setting from the Grid. After you create zones in the DNS view, Grid Manager can then determine the associated members and display the resulting inheritance. If a DNS view has multiple zones served by multiple members with different recursion settings, you can view the different settings in the Multi-Inheritance viewer.
- A comment. You can enter up to 256 characters.

This setting overrides the recursion setting at the Grid and member levels.

To configure a new DNS view:

1. If there is more than one network view in the Grid, select the network view in which you are creating the DNS view.
2. From the Data Management tab -> DNS tab, expand the Toolbar and click Add -> Add DNS View.
3. In the Add DNS View wizard, complete the following fields:
   - DNS View: Enter the name of the DNS view. It can be up to 64 characters long and can contain any combination of printable characters. Each DNS view must have a unique name. You cannot create two DNS views with the same name, even if they are in different network views.
   - Comment: Optionally, enter information about the DNS view. You can enter up to 256 characters.
   - Enable Recursion: This field's initial default state is inherited from the Grid. It is inactive and greyed out until you click Override. After you click override, you can select or clear the check box to define a setting that applies to the DNS view only. Note that a DNS view actually inherits its recursion setting from the Grid members that serve its zones. When you first create a DNS view though, it does not have any zones and therefore inherits its setting from the Grid. After you create zones in the DNS view, Grid Manager can then determine the associated members and display the resulting inheritance. If a DNS view has multiple zones served by multiple members with different recursion settings, you can view the different settings in the Multi-Inheritance viewer.
   - Inherit: Select this check box to disable this DNS view.
4. Save the configuration and click Restart if it appears at the top of the screen, or click Next to define a Match Clients list. For information, see Defining Match Clients Lists.
Defining Match Clients Lists

When you configure a DNS view, you can create a Match Clients list to identify source IP addresses and TSIG keys that are allowed or denied access to the DNS view. The NIOS appliance determines which hosts can access a DNS view by matching the source IP address or TSIG key with its Match Clients list. After the appliance determines that a host can access a DNS view, it checks the zone level settings to determine whether it can provide the service that the host is requesting for that zone.

If you do not configure a Match Clients list, then all devices are allowed access to the DNS view. However, if you configure a Match Clients list, then only those devices in the list with "Allow" permission can access the DNS view. All other devices are denied access, including Grid members. Therefore, to allow a primary server of a zone to receive dynamic DNS updates from member DHCP servers, you must add the members to the Match Clients list as well. Note that if you "Deny" permission to certain IP addresses or networks, you must add the "Allow Any" permission at the end of the Match Clients list to ensure that all other IP addresses and networks that are not in the "Deny" list are allowed access to the DNS view.

You can add individual ACEs (access control entries) or a named ACL (access control list) to the Match Clients list. For information about named ACLs and how to define them, see Defining Named ACLs.

Defining a Match Clients List for a DNS View

You can define a Match Clients list for a DNS view when you add a new DNS view (second step of the Wizard) or when you edit an existing DNS view. For information about adding a DNS view, see Adding a DNS View. To define a Match Clients list for an existing DNS view:

1. From the Data Management tab, click the DNS tab > Zones tab> dns_view check box -> Edit icon. Or, if there is only one DNS view, for example the predefined default view, you can just click the Edit icon beside it.

2. In the DNS View editor, select the Match Clients tab, and select one of the following:
   - **None**: Select this if you do not want to configure a Match Clients list. The appliance allows all clients to access the DNS view. This is selected by default.
   - **Named ACL**: Select this and click Select Named ACL to select a named ACL. Grid Manager displays the Named ACLs Selecto r. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this option, the appliance allow access to the DNS view from sources that have the Allow permission in the named ACL. You can click Clear to remove the selected named ACL.
   - **Set of ACEs**: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding.
     - **IPv4 Address** and **IPv6 Address**: Select this to add an IPv4 address or IPv6 address. Click the Value field and enter the IP address. The Permission column displays **Allow** by default. You can change it to **Deny** by clicking the field and selecting **Deny** from the drop-down list.
     - **IPv4 Network**: In the Add IPv4 Network panel, complete the following, and then click **Add** to add the network to the list:
       - **Address**: Enter an IPv4 network address and either a netmask or move the slider to the desired netmask.
       - **Permission**: Select **Allow** or **Deny** from the drop-down list.
     - **IPv6 Network**: In the Add IPv6 Network panel, complete the following, and then click **Add** to add the network to the list:
       - **Address**: Enter an IPv6 network address and select the netmask from the drop-down list.
       - **Permission**: Select **Allow** or **Deny** from the drop-down list.
     - **TSIG Key**: In the Add TSIG Key panel, complete the following, and then click **Add** to add the TSIG key to the list:
       - **Key name**: Enter a meaningful name for the key, such as a zone name or the name of the client or Grid member. This name must match the name of the same TSIG key on other name servers.
       - **Key Algorithm**: Select either HMAC-MD5 or HMAC-SHA256.
       - **Key Data**: To use an existing TSIG key, type or paste the key in the Key Data field. Alternatively, you can select the key algorithm, select the key length from the Generate Key Data drop down list, and then click **Generate Key Data** to create a new key.
     - **DNSOne 2.x TSIG Key**: Select this when the other name server is a NIOS appliance running DNS One 2.x code. The appliance automatically populate the value of the key in the Value field. The Permission column displays **Allow** by default. You cannot change the default permission.
     - **Any Address/Network**: Select this to allow or deny any IP addresses to access the DNS view.
   - **Add** to add the selected named ACL.

3. Save the configuration and click **Restart** if it appears at the top of the screen. You can also click the Schedule icon at the top of the editor to schedule this task. In the Schedule Change panel, enter a date, time, and time zone.

Defining a Match Destinations List

Copyright ©2019, Infoblox, Inc. All right reserved.
You can define a Match Destinations list that identifies destination addresses and TSIG keys that are allowed access to a DNS view. When the NIOS appliance receives a DNS request from a client, it tries to match the destination address or TSIG key in the incoming message with its Match destination list to determine which DNS view, if any, the client can access. After the appliance determines that a host can access a DNS view, it checks the zone level settings to determine whether it can provide the service that the host is requesting for that zone.

You can define a Match Destination list when you edit an existing DNS view as follows:

1. From the Data Management tab, click the DNS tab > Zones tab> dns_view check box -> Edit icon. Or, if there is only one DNS view, for example the predefined default view, you can just click the Edit icon beside it.
2. In the DNS View editor, select the Match Destinations tab, and select one of the following:
   - None: Select this if you do not want to configure a Match Destinations list. The appliance allows all destination addresses to access the DNS view. This is selected by default.
   - Named ACL: Select this and click Select Named ACL to select a named ACL. Grid Manager displays the Named ACLs Select option. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this option, the appliance allows access to the DNS view from the destination addresses that have the Allow permission in the named ACL. You can click Clear to remove the selected named ACL.
   - Set of ACEs: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list.
     - IPv4 Address and IPv6 Address: Select this to add an IPv4 address or IPv6 address. Click the Value field and enter the IP address. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.
     - IPv4 Network: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
       - Address: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
       - Permission: Select Allow or Deny from the drop-down list.
     - IPv6 Network: In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
       - Address: Enter an IPv6 network address and select the netmask from the drop-down list.
       - Permission: Select Allow or Deny from the drop-down list.
     - TSIG Key: In the Add TSIG Key panel, complete the following, and then click Add to add the TSIG key to the list:
       - Key name: Enter a meaningful name for the key, such as a zone name or the name of the client or Grid member. This name must match the name of the same TSIG key on other name servers.
       - Key Algorithm: Select either HMAC-MD5 or HMAC-SHA256.
       - Key Data: To use an existing TSIG key, type or paste the key in the Key Data field. Alternatively, you can select the key algorithm, select the key length from the Generate Key Data drop down list, and then click Generate Key Data to create a new key.
   - DNSone 2.x TSIG Key: Select this when the other name server is a NIOS appliance running DNS One 2.x code. The appliance automatically populates the value of the key in the Key field. The Permission column displays Allow by default. You cannot change the default permission.
   - Any Address/Network: Select this to allow or deny any IP addresses to access the DNS view.
     - After you have added access control entries, you can do the following:
       - Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL icon and enter a name in the Convert to Named ACL dialog box. The appliance creates a new named ACL and adds it to the Named ACL panel. Note that the ACEs you configure for this operation stay intact.
       - Reorder the list of ACEs using the up and down arrows next to the table.
       - Select an ACE and click the Edit icon to modify the entry.
       - Select an ACE and click the Delete icon to delete the entry. You can select multiple ACEs for deletion.
3. Save the configuration and click Restart if it appears at the top of the screen. You can also click the Schedule icon at the top of the editor to schedule this task. In the Schedule Change panel, enter a date, time, and time zone.

Enabling the Match Recursive Only Option

You can enable the match-recursive-only option for the DNS view. When you enable this option, only recursive queries from matching clients match the selected DNS view. This option can be used in conjunction with the match client list and match destination list. Ensure that you configure those options and the order of the DNS views accordingly if you want to also enable the match-recursive-only option.

To enable the match-recursive-only option, complete the following:

1. From the Data Management tab, click the DNS tab > Zones tab> dns_view check box -> Edit icon. Or, if there is only one DNS view, for example the predefined default view, you can just click the Edit icon beside it.
2. In the DNS View editor, select the General tab -> Advanced tab, and select the following:
   - Enable match recursive only option: This option is disabled by default. Select this option to enable the match-recursive-only option for the DNS view. When you select this option, only recursive queries from matching clients match this view. Note that this option can be used in conjunction with the match-clients and match-destinations options. Ensure that you configure those options and the order of the DNS views accordingly if you want to also enable match-recursive-only.
3. Save the configuration.

Note: You can also enable or disable the match-recursive-only option for a specific DNS view on a specific member by using the CLI command set enable_match_recursive_only. For information about this command, refer to the Infoblox CLI Guide.
Copying Zone Records

Different views of the same zone may have a number of records in common. If this is the case, you can copy zone records between views and zones.

Note: You cannot copy shared records and records that the NIOS appliance automatically creates, such as NS records and glue A records.

To copy zone records between DNS zones and views:

1. From the Data Management tab -> DNS tab, click Copy Records from the Toolbar.
2. In the Copy Records dialog box, Grid Manager displays the last selected zone or the zone from which you are copying zone records in the Source field. Complete the following to copy records:
   - **Destination:** Select Zone to select the destination zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box from which you can select one. After you select the zone, Grid Manager displays the associated DNS view.
   - **Copy All records:** Select this option to copy all the zone records, including those records not created on the NIOS appliance, such as HINFO records.
   - **Copy Specific Records:** Select this option to copy specific types of records. Select a resource record type from the Available Specific Records column and click the right arrow to move it to the Selected column.
   - **Copy Options:** Select one of the following:
     - Delete all records in destination before copying the records: Select to delete all resource records in the destination zone before the records are copied.
     - Overwrite existing records: Select to overwrite existing resource records that have the same domain name owners as the records being copied.
3. Click Copy & Close.

Note: When you copy resource records between zones and there are pending scheduled tasks associated with these records, the appliance allows the copying of zone records before it executes the scheduled tasks.

Managing the DNS Views of a Grid Member

A Grid member can serve zones in different DNS views. You can manage the DNS views associated with a Grid member as follows:

- You can specify which interface IP address is published in glue A records in the DNS view, as described in Changing the Interface IP Address.
- You can assign an empty recursive view to a member, as described in Managing Recursive DNS Views.
- You can control the list of DNS views as described in Changing the Order of DNS Views.

Changing the Interface IP Address

By default, a Grid member publishes its LAN address in glue A records in the DNS view. You can change this default for each DNS view associated with a member. You can specify the NAT IP address or another IP address.

To specify the interface IP address for glue A records in a view:

1. From the Data Management tab, click the DNS tab -> Members tab -> member check box, and then click the Edit icon.
2. In the Member DNS Configuration editor, click Toggle Expert Mode if the editor is in basic mode, and then select the DNS Views tab.
   - The Address Of Member Used in DNS Views table lists the default DNS view and DNS views with zones that are served by the member.
3. To change the address, click the entry in the Interface column of a DNS view, and select one of the following:
   - **NAT IP Address:** Select this to use the member NAT address for glue A records in a Grid setting. Select this when you want to notify the Grid Master that it should expect packets from this member on the NAT address, not the configured interface address. The Grid Master broadcasts this NAT address to all NAT members outside of its NAT group. Do not use this option for an independent appliance serving as a DNS server. Select Other IP Address to publish the NAT address for the independent appliance. For information about NAT compatibility, see NAT Groups.
   - **Other IP Address:** Select this to specify another address for glue A records, or to publish the NAT address for an independent appliance. Enter the address in the Address field.

   Note: The 255.255.255.255 limited broadcast address is reserved. The appliance does not automatically create glue A records for this address. You can however create an NS record without the associated glue records.

4. Save the configuration and click Restart if it appears at the top of the screen.

Managing Recursive DNS Views

When you add a DNS view that has recursion enabled, the appliance resolves recursive queries from hosts on the Match Clients list of that view. If the DNS view contains zones and you delete those zones, the appliance retains the view in its configuration file, as long as recursion is enabled in the view. Such a view is called an empty recursive DNS view because it does not contain any zones. It enables the appliance to respond to
In a Grid, all members automatically store DNS views that have recursion enabled in their configuration files. If you do not want a Grid member to respond to recursive queries for clients in a particular DNS view, you can remove the view from the member’s configuration file.

To delete or retain an empty recursive DNS view in the DNS configuration file of a Grid member:

1. From the Data Management tab, click the DNS tab > Members tab> Grid_member check box -> Edit icon.
2. In the Member DNS Configuration editor, click Toggle Expert Mode if the editor is in basic mode, and then select the DNS Views tab.
3. The Recursive Views Assigned to this Member section lists the empty recursive DNS views. Move a DNS view to the Selected column to explicitly assign the view to the Grid member and include it in the DNS configuration file of the member. Move a DNS view to the Available column to remove it from the configuration file of the member.

Empty recursive DNS views that you retain in the configuration file are automatically listed at the bottom of the list of DNS views. You can move them up on the list when you manually change the order of the DNS views, as described in Managing the DNS Views of a Grid Member.

4. Save the configuration and click Restart if it appears at the top of the screen.

Managing the Order of DNS Views

When a member receives a query from a DNS client, it checks the Match Client lists in the order the DNS views are listed in the Order of DNS Views table of the DNS Views tab in the DNS Member editor. The NIOS appliance can order DNS views automatically, or you can order the DNS views manually. If you choose to have the appliance automatically update the order of the DNS views, it does so after each of the following events:

- Adding a DNS view to a member.
- Removing a DNS view from a member.
- Changing the address match list of a DNS view hosted by the member.

About IP Addresses and the Order of DNS Views

NIOS appliances with both IPv4 and IPv6 enabled can contain both types of addresses in the Match Clients list. When you enable IPv6 on the appliance, the order of DNS views in the GUI may be affected. Views are ordered and sorted automatically based on Match Clients lists. Views with IPv6 enabled are sorted as follows:

- If the Match Clients lists of all views contain IPv4 addresses only—The appliance orders views based on IPv4 addresses.
- If the Match Clients lists of all views contain IPv6 addresses only—The appliance orders views based on IPv6 addresses.
- If the Match Clients list of one DNS view has IPv4 addresses and all other views have IPv4 addresses—The appliance orders views based on IPv4 addresses, and the IPv6 address is given lowest priority in the ordering.
- If the Match Clients list of one DNS view has IPv4 addresses and all other DNS views have IPv6 addresses—The appliance orders DNS views based on IPv6 addresses, and the IPv4 address is given lowest priority in the ordering.
- If the Match Clients list of one DNS view has both IPv4 and IPv6 addresses—The appliance orders DNS views based on both IPv4 and IPv6 addresses, but more priority is given to the IPv4 addresses in the ordering.

The DNS views are ordered based on the number of IP addresses that are matched by the Access Control Lists (ACLs). The order of the DNS view is as follows:

- ANY
- Large Network
- Small Network
- Multiple Addresses
- Single Address

The actual precedence of the order of the views is also based on the ACL elements:

- any match: precedence = UINT_MAX + 1
- address match: precedence += 1
- TSIG match: precedence += 1
- network match: precedence += 129 - split (BOTH v4 and v6)

Note that views with the same precedence are sorted based on the internal view name. For example, '_default' or '0'.

**Note:** Only superusers can change the order of the views.

Changing the Order of DNS Views

To change the order of DNS views:

1. From the Data Management tab, click the DNS tab > Members tab> Grid_member check box -> Edit icon.
2. In the Member DNS Configuration editor, click Toggle Expert Mode if the editor is in basic mode, and then select the DNS Views tab.
3. In the Order of DNS Views section, select one of the following:
   - Order DNS Views Automatically: Click this to automatically order views after adding a new DNS view, removing a DNS view,
or changing the match client list.

- **Order DNS Views Manually**: This able lists the DNS views that have zones assigned to the Grid member and the empty recursive views associated with the member. Select a DNS view, then click an arrow to move it up or down in the list.

4. Save the configuration and click Restart if it appears at the top of the screen.

**Managing DNS Views**

You can list the DNS views, and then modify, disable, or remove any custom DNS view. You can modify and disable the default DNS view; however, under no circumstances can it be removed.

**Listing DNS Views**

After you configure additional DNS views, you can list all DNS views by navigating to the Data Management tab -> DNS tab -> Zones panel. This panel lists DNS views only after you modify the default DNS view or add a DNS view. If you never added DNS views or modified the default DNS view, this panel does not display the default DNS view. Instead, it lists the zones in the default DNS view. To display the properties of the default DNS view and edit it, use the Global Search function to locate and edit it.

Note that if you have not used Grid Manager to add a new DNS view, and you import DNS views through the Data Import Wizard or the API, you must log out and log back in to Grid Manager to display the newly imported DNS views.

For each DNS view, this panel displays the following by default:

- **Comment**: Comments that were entered for the DNS view.
- **Site**: Values that were entered for this pre-defined attribute. You can also display the following column:
- **Disabled**: Indicates if the DNS view is enabled or disabled. Disabled DNS views are excluded from the named.conf file.

From this list, you can do the following:

- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
- List the zones in a DNS view by clicking a DNS view name.
- Edit information about a DNS view, as described in the next section.
- Delete a DNS view, as described in Deleting DNS Views.

**Modifying DNS Views**

To modify a DNS view:

1. From the Data Management tab, click the DNS tab > Zones tab> dns_view check box -> Edit icon.
2. In the DNS View editor, you can do the following:
   - In the General tab, you can change any of the information you entered through the wizard. You can also disable a DNS view to temporarily block access to a DNS view. Disabling a DNS view excludes it from the named.conf file. For a description of the fields, see the online Help or Configuring DNS Views.
   - In the Match Clients tab, define or update a Match Clients list, as described in Defining Match Clients Lists.
   - In the Match Destinations tab, define or update match destinations, as described in Defining a Match Destinations List.
   - In the Forwarders tab, configure forwards for the view, as described in Using Forwarders.
   - In the Queries tab, enable AAAA filtering and configure a list of IPv4 networks and addresses for allowing or denying AAAA filtering, as described in Enabling AAAA Filtering.
   - In the DNSSEC tab, you can specify parameters for DNSSEC as described in Configuring DNSSEC on a Grid.
   - In the Root Name Servers tab, you can configure root name servers, as described in About Root Name Servers.
   - In the Sort List tab, define a sort list for the DNS view, as described in Defining a Sort List.
   - In the Blacklist tab, define blacklist rulesets, as described in Enabling Blacklisting.
   - In the Extensible Attributes tab, you can modify the attributes. For information, see Using Extensible Attributes.
   - The Permissions tab displays if you logged in as a superuser. For information, see About Administrative Permissions.
   - In the Record Scavenging tab, define the rules for DNS records scavenging in the DNS view, as described in Configuring DNS Record Scavenging Properties.
   - In the Updates tab, specify the secure dynamic updates settings, as described in Secure Dynamic Updates.
   - Save the configuration and click Restart if it appears at the top of the screen.

3. Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

**Deleting DNS Views**

You can delete a DNS view if it is not the only view associated with a network view and if it is not selected for dynamic DNS updates. You cannot remove the system-defined default DNS view. When you remove a DNS view, the NIOS appliance removes the forward and reverse mappings of
all the zones defined in the DNS view.

To delete a DNS view:

- From the Data Management tab, select the > DNS tab> Zones tab> dns_view check box.

To delete the DNS view immediately, click the Delete icon, and then click Yes to confirm the delete request. To schedule the deletion, click Schedule Deletion and in the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Deletions.

Grid Manager moves the view to the Recycle Bin, from which you can restore or permanently delete it.

Configuration Example: Configuring a DNS View

In Figure 18.4, Member-A is a member of a Grid. It is the primary name server for the corpxyz.com zone in the internal DNS view. It allows the IP address 192.168.10.1 and the 10.2.2.0/24 subnet access to DNS zone data in the internal DNS view. At the zone level, it allows transfers to an external secondary server, Infoblox-B, with an IP address of 192.168.10.1. Infoblox-B is a secondary server for the corpxyz.com zone. The process follows these steps:

1. Adding an Internal DNS View on Member-A
2. Adding a Zone to a DNS View
3. Copying Records Between DNS Zones from the corpxyz.com zone in the default DNS view to the corpxyz.com zone in the internal DNS view
4. Verifying the Configuration

Figure 18.4 Configuring a DNS View

Adding an Internal DNS View

1. Expand the Toolbar and click Add -> Add DNS View.
2. In the Add DNS View wizard, specify the following, and then click Next:
   - Name: internal
   - Comment: internal DNS view
3. In the Match Clients panel, click Add and select IPv4 Network from the drop-down list.
4. Do the following for IP addresses in the network 10.2.2.0/24:
   - Enter 10.2.2.0/24 in the in the Address field.
   - The Permission field displays Allow by default. Leave it as is.
   - Click Add.

You will have 255 allowed client addresses in the Match Clients list when you are done.
5. Save the configuration and click Restart if it appears at the top of the screen.

Adding a Zone to a DNS View

1. Expand the Toolbar and click Add -> Zone -> Add Auth Zone.
2. In the Add Auth Zone wizard, click Add an authoritative forward-mapping zone and click Next.
3. Specify the following, and then click Next:
   b. DNS View: Select Internal from the drop-down list.
4. In step 3 of the wizard, do the following:
   a. Select Use this set of name servers.
   b. Click the Add icon and select Grid Primary.
   c. Click Select Member and select Member A from the Select Grid Member dialog box.
   d. Click Add to add the Grid member to the list of name servers.
   e. Click the Add icon again and select External Secondary.
   f. Enter the following information, and then click Add:
      - Name: InfobloxB
      - IP Address: 192.168.10.1
5. Click Save & Edit to display the Authoritative Zone editor and continue with the zone configuration.
6. Click Queries.
7. Click Override, and then click the Add icon and select IPv4 Network.
   a. Enter 10.2.2.0/8 in the in the Address field.
   b. The Permission field displays Allow by default. Leave it as is.
   c. Click Add.
8. This allows queries that the appliance answers from its internal DNS view.
9. Save the configuration and click Restart if it appears at the top of the screen.

Copying Records Between DNS Zones

1. Navigate to the default DNS view and select the corpxyz.com zone.
2. Expand the Toolbar and click Copy Records.
3. In the Destination field, click Select Zone, and then select the corpxyz.com zone in the Internal DNS view.
4. Select Copy all records, and then click OK.
5. Save the configuration and click Restart if it appears at the top of the screen.

The records from corpxyz.com in the default DNS view are copied to corpxyz.com in the internal DNS view.

Note: Only superusers can copy A, AAAA, shared A, and shared AAAA records with a blank name. Limited-access users must have read/write permission to Adding a blank A/AAAA record in order to copy A, AAAA, shared A, and shared AAAA records with a blank name, otherwise the copying records operation might fail. You can assign global permission for specific admin groups and roles to allow to copy A, AAAA, shared A, and shared AAAA records with a blank name. For more information, see Administrative Permissions for Adding Blank A or AAAA Records.

Verifying the Configuration

1. In the DNS tab, click Members and select the Member-A check box.
2. Expand the Toolbar and click View -> View DNS Configuration.
3. In the DNS Configuration File viewer, scroll through the contents of the file.

Verify that the internal DNS view section is similar to the configuration file shown.

Chapter 19 Configuring DNS Zones

This chapter provides general information about DNS zones that you can configure and manage on the Infoblox appliance. The topics in this chapter include:

- About Authoritative Zones
- Configuring Authoritative Zones
  - Creating an Authoritative Forward-Mapping Zone
  - Creating an Authoritative Reverse-Mapping Zone
  - Creating a Root Zone
  - Adding an Authoritative Subzone
  - Locking and Unlocking Zones
  - Enabling and Disabling Zones
- Removing Zones
- Configuring Authoritative Zone Properties
- IDN Support For DNS Zones
- About DNS Integrity Check for Authoritative Zones
- Configuring DNS Integrity Check
About Authoritative Zones

An authoritative zone is a zone for which the local (primary or secondary) server references its own data when responding to queries. The local server is authoritative for the data in this zone and responds to queries for this data without referencing another server.

There are two types of authoritative zones:

- **Forward-mapping** – An authoritative forward-mapping zone is an area of domain name space for which one or more name servers have the responsibility to respond authoritatively to name-to-address queries.
- **Reverse-mapping** – A reverse-mapping zone is an area of network space for which one or more name servers have the responsibility to respond to address-to-name queries.

Configuring Authoritative Zones

You can configure and manage authoritative forward-mapping and IPv4 and IPv6 reverse-mapping zones on an Infoblox appliance. In a Grid, an authoritative forward-mapping zone is an area of domain name space for which one or more Grid members have the responsibility to respond authoritatively to name-to-address queries. The Grid members can function as primary or secondary servers for the zone.

You can add arpa as the top-level forward-mapping zone and manage its resource records. You can also add in-addr.arpa (for ipv4 addresses) and ip6.arpa (for ipv6 addresses) as the top-level reverse-mapping zones. You can create these top-level reverse-mapping zones under an arpa or a root parent forward-mapping zone or without a parent zone. If you want arpa, in-addr.arpa, and ip6.arpa zones on the appliance, you must manually create them. These zones are not auto-created.

Sample IPv4 reverse-mapping zone hierarchy:
```
. (root zone) > arpa > in-addr.arpa > 10.in-addr.arpa
```

Sample IPv6 reverse-mapping zone hierarchy:
```
. (root zone) > arpa > ip6.arpa > a.ip6.arpa
```

Following are the tasks to configure an authoritative zone:

1. Create the zone. The following sections explain how to create authoritative forward-mapping zones, reverse-mapping zones, subzones, and a custom root zone:
   - **Creating an Authoritative Forward-Mapping Zone**
   - **Creating an Authoritative Reverse-Mapping Zone**
   - **Creating a Root Zone**

2. Assign an Infoblox appliance as the primary or secondary server of the zone. For information, see Assigning Zone Authority to Name Servers.

3. Import resource records or add resource records manually. The following provides information about resource records:
   - **Managing Resource Records**
   - **Importing Zone Data**

4. Configure additional parameters. For information, see Configuring Authoritative Zone Properties.

5. Optionally, associate the zone with one or more networks. This is useful when you want to restrict the A, AAAA and host records to IP addresses from specific networks. For information, see Associating Networks with Zones.

Creating an Authoritative Forward-Mapping Zone

An authoritative forward-mapping zone is an area of domain name space for which one or more Grid members have the responsibility to respond authoritatively to name-to-address queries.

**Note:** A single forward-mapping zone can map names to both IPv4 and IPv6 addresses.
To create an authoritative forward-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar, and click Add -> Zone -> Add Auth Zone.
2. In the Add Authoritative Zone wizard, click Add an authoritative forward-mapping zone and click Next.
3. Specify the following:
   - Name: Enter the domain name for the zone. Omit the trailing period (".") that signifies the root zone. You can use IDNs as well.
   - DNS View: This field displays only when there is more than one DNS view in the current network view. Select a DNS view from the drop-down list.
   - Comment: Enter a descriptive comment about the zone.
   - Lock: Click this check box to lock the zone so that you cannot make changes to it and prevent others from making conflicting changes. For information, see Locking and Unlocking Zones.
4. Save the configuration, or click Next to continue to the next steps in the wizard as follows:
   - Define the name servers for the zone. For information on specifying primary and secondary servers, see Assigning Zone Authority to Name Servers. For information on specifying authoritative name server groups, see Using Authoritative Name Server Groups.
   - If you have assigned a Microsoft server as the primary server for the zone and if the zone is AD-integrated, you can configure a list of domain controllers that are allowed to add NS records to the zone. For information see, Configuring Domain Controller List.
   - Define extensible attributes. For information, see Using Extensible Attributes.
5. Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.
6. Click Restart if it appears at the top of the screen.

Creating an Authoritative Reverse-Mapping Zone

An authoritative reverse-mapping zone is an area of network space for which one or more name servers—primary and secondary—have the responsibility to respond to address-to-name queries. Infoblox supports reverse-mapping zones for both IPv4 and IPv6 addresses. You can add in-addr.arpa and ip6.arpa as the top-level reverse-mapping zones. Note that you cannot add these zones using their IP addresses or netmasks, however, you can add them by name "in-addr.arpa" and "ip6.arpa" respectively.

Specifying an RFC 2317 Prefix

RFC 2317, Classless IN-ADDR.ARPA delegation is an IETF (Internet Engineering Task Force) document that describes a method of delegating parts of the DNS IPv4 reverse-mapping tree that correspond to subnets smaller than a /24 (from a /25 to a /31). The DNS IPv4 reverse-mapping tree has nodes broken at octet boundaries of IP addresses, which correspond to the old classful network masks. So, IPv4 reverse-mapping zones (and delegation points) usually fall on /8, /16, or /24 boundaries.

With the proliferation of CIDR (Classless Inter-Domain Routing) support for routing, ISPs no longer assign entire /24 networks to customers that only need a handful of IPv4 addresses. In general, IPv4 address assignments no longer fall on classful boundaries. For DNS, a problem comes into play when an ISP gives a customer an address range that is smaller than a /24, but the customer also wants to be delegated the DNS reverse-mapping zone.

If the ISP gives you, for example, a subnet with a 25-bit mask, then you only have half of the /24 address range. If you configure your DNS server to be authoritative for the zone corresponding to a /24 subnet, the DNS server cannot resolve half of the possible reverse-mapping records in the zone. RFC 2317 defines an approach, considered a best practice, which addresses this issue.

In addition to IPv4 reverse-mapping zones, you can also configure IPv4 reverse-mapping delegation zones that have an RFC2317 prefix. For more information about configuring a delegation for a reverse-mapping zone, see Configuring a Delegation.

Note: Before enabling RFC 2317 support for zones, disable forwarders for the zone, especially when any sort of delegation (including RFC 2317) is being used. If you do not, reverse lookups may fail. For more information, contact Infoblox Support for the Tech Note on RFC 2317 delegation.

Adding an IPv4 Reverse-Mapping Zone

To add an IPv4 reverse-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Auth Zone.
2. In the Add Authoritative Zone wizard, click Add an authoritative IPv4 reverse-mapping zone and click Next.
3. Specify the following zone information:
   - IPv4Network: Enter the IPv4 address for the address space for which you want to define the reverse-mapping zone and select a netmask from the Netmask drop-down list. Alternatively, you can specify the address in CIDR format, such as 192/8.
     To use an RFC 2317 prefix, select a netmask value that is between 25 to 31, inclusive. Grid Manager displays the RFC2317Prefix field. Enter a prefix in the text field. Prefixes can include alphanumeric characters. For information, see Specifying an RFC 2317 Prefix.
   - Name: Enter the domain name of the reverse-mapping zone.
   - DNS View: This field displays only when there is more than one DNS view in the current network view. Select a DNS view from the drop-down list.

Copyright ©2019, Infoblox, Inc. All right reserved.
• **Comment:** Optionally, enter additional information about the zone.
• **Disable this zone:** Select this option to temporarily disable this zone. For information, see *Enabling and Disabling Zones.*
• **Lock this zone:** Select this option to lock the zone so that you can make changes to it and prevent others from making conflicting changes. For information, see *Locking and Unlocking Zones.*

4. Save the configuration, or click **Next** to continue to the next steps in the wizard as follows:

   • Define the name servers for the zone. For information on specifying primary and secondary servers, see *Assigning Zone Authority to Name Servers.* For information on specifying authoritative name server groups, see *Using Authoritative Name Server Groups.*
   
   • If you have assigned a Microsoft server as the primary server for the zone and if the zone is AD-integrated, you can configure a list of domain controllers that are allowed to add NS records to the zone. For information see, *Configuring Domain Controller List.*
   
   • Define extensible attributes. For information, see *Using Extensible Attributes.*

   or Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see *Scheduling Tasks.*

5. Click **Restart** if it appears at the top of the screen.

### Adding an IPv6 Reverse-Mapping Zone

To add an IPv6 reverse-mapping zone:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Add** -> **Zone** -> **Add Auth Zone**.
2. In the **Add Authoritative Zone** wizard, click **Add an authoritative IPv6 reverse-mapping zone** and click **Next**.
3. Enter the following zone information:
   
   • Enter one of the following to identify the zone:
     
     - **IPv6NetworkPrefix:** Enter the 128-bit IPv6 address for the address space for which you want to define the reverse-mapping zone. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006::0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab::cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered. Choose the network prefix that defines the IPv6 network address space.
     
     - **Name:** Enter the domain name of the reverse-mapping zone.
   
   • **DNS View:** This field displays only when there is more than one DNS view in the current network view. Select a DNS view from the drop-down list.
   
   • **Comment:** Enter a descriptive comment about the zone.
   
   • **Disable:** Click this check box to temporarily disable this zone. For information, see *Enabling and Disabling Zones.*
   
   • **Lock:** Click this check box to lock the zone so that you can make changes to it and prevent others from making conflicting changes. For information, see *Locking and Unlocking Zones.*

4. Save the configuration, or click **Next** to continue to the next steps in the wizard as follows:

   • Define the name servers for the zone. For information on specifying primary and secondary servers, see *Assigning Zone Authority to Name Servers.* For information on specifying authoritative name server groups, see *Using Authoritative Name Server Groups.*
   
   • Define extensible attributes. For information, see *Using Extensible Attributes.*

   or Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see *Scheduling Tasks.*

### Creating a Root Zone

The NIOS appliance allows you to create an internal root zone for your organization. When the appliance receives a query for DNS data that is not in its cache or authoritative data, it can query an internal root server after querying any specified forwarders. If you do not specify an internal root server and the appliance can access the Internet, it queries the Internet root servers. For information on root name server, see *About Name Servers.*

To create a root zone, create an authoritative forward-mapping zone as described in *Creating an Authoritative Forward-Mapping Zone* and specify the following:

• Enter a period (.) in the **Name** field.

• Optionally, enter a comment.

• Select a Grid member as the primary name server for the root zone.

Once created, the root zone automatically becomes the parent of all the zones under the root zone.

### Adding an Authoritative Subzone

After creating a zone, you can add more zones at the same level, or add subordinate zones (*subzones*). The subzones can be authoritative, delegated, forward, or stub. For simplicity, the zones created in this example are authoritative (as are all zones by default). For information about configuring the other zone types, see *Configuring Delegated, Forward, and Stub Zones.*

You create an authoritative zone when you assign authority for all the resource records of a particular domain to one or more name servers. You create a subzone when you assign authority for all the resource records of a subdomain to name servers. The name servers can be the same as, or different from, the name servers that serve resource records for the parent domain.

The distinction between domains and zones is that domains provide a logical structure to the DNS name space while zones provide an administrative structure. The difference between domains and subdomains and zones and subzones is that the terms *subdomains and subzones*
reference their relationship to a parent domain or zone. With the exception of the root domain and root zone, all domains are subdomains and all zones are subzones.

You can organize a domain based on logical divisions such as type (.com, .gov, .edu; or sales, eng, sup) or location (.uk, .jp, .us; or hq, east, west). Figure 19.1 shows one way to organize the external (public) name space and the internal (private) name space for a corporation with the domain name corp.xyz.com. The external name space follows standard DNS conventions. Internally, you create an individual subdomain and corresponding subzone for each department.

Figure 19.1 Domains and Subdomains, and Forward-Mapping Zones and Subzones

The DNS name space is logically structured into domains and subdomains. The DNS name space is administratively structured into zones and subzones.

The procedure for adding a subzone is the same as that used to add an authoritative zone. The only difference is that you specify the subzone name in the Name field. For information about adding authoritative zones, see Configuring Authoritative Zones.

Locking and Unlocking Zones

You can lock a zone when you create or edit it to prevent other administrators from making conflicting changes. When you lock a zone, Grid Manager displays LOCKED beside the zone name when you view the records and subzones of the zone in the Zones panel. When other administrators try to make changes to a locked zone, the system displays a warning message that the zone is locked by admin_name.

You can perform dynamic updates through mechanisms such as DDNS and nsupdate on a locked zone. The system can also add auto-generated records such as glue A records and NS records to a locked zone. Locks on a zone do not impact its child zones.

Only a superuser or the administrator who locked the zone can unlock it. Locks do not expire; you must manually unlock a locked zone.

Enabling and Disabling Zones

The NIOS appliance allows you to disable and enable a zone when you create or edit it. When you disable a zone, Grid Manager removes it from the DNS configuration file, but not from the database. This feature is especially helpful when you have to move or repair the server for a particular zone. You can easily disable a zone temporarily, and then enable it after the move or repair is completed.

Note: When you temporarily disable a zone that has an associated NS group, the appliance removes all the automatically generated NS records, glue A or AAAA records, and PTR records from the zone. The appliance automatically generates the NS records, glue A or AAAA records, and PTR records when you re-enable the zone.

Configuring Authoritative Zone Properties

A zone inherits some of its properties from the Grid or from the member that serves it as a primary or secondary server. When you edit a zone, you can override properties set at the Grid or member level and modify the original zone settings, as well.

To configure authoritative zone properties:

1. From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and then click the Edit icon.
2. In the Authoritative Zone editor, you can do the following in each tab:
   - **General**: Modify the original zone settings, except the zone name.
   - **Name Servers**: Specify primary and secondary servers as described in Assigning Zone Authority to Name Servers.
• **Settings:** Set certain properties if the primary server is a Grid member. If the zone's primary server is an external server, then all these fields, except *Don't use forwarders to resolve queries in subzones*, are read-only with the information derived from the SOA record of the zone.
  - The **Serial Number** field displays the zone's current serial number. You can change the serial number in an SOA record only if the primary server of the zone is a Grid member. The serial number in the SOA record increments every time the record is modified. This serial number plays a key role when and how zone data is updated via zone transfers. The NIOS appliance allows you to change the serial number (in the SOA record) for the primary server so it is higher than the secondary server, thereby ensuring zone transfers come from the primary server (as they should).
  - Override the Grid or member TTL settings as described in *About Time To Live Settings*.
  - Override the email settings, as described in *Adding an Email Address to the SOA Record*.
  - Change the primary name server that is specified in the SOA MNAME of a zone, as described in *Changing the SOA Name for a Zone*.
  - **Don't use forwarders to resolve queries in subzones:** If the DNS members are configured to use forwarders to resolve queries that they cannot resolve locally, you can select this check box to disable the use of forwarders to resolve queries for data in the subzones.

• **Queries:** Set restrictions for queries as described in *Controlling DNS Queries*.

• **Zone Transfers:** Specify to which servers zone transfers are allowed as described in *Enabling Zone Transfers*.

• **Updates:** Set dynamic DNS update properties as described in *Configuring DNS Servers for DDNS*.

• **Active Directory:** Set parameters to allow zones to receive GSS-TSIG authenticated DDNS updates from DHCP clients and servers in an AD domain. For information, see *Supporting Active Directory*.

• **Extensible Attributes:** Define extensible attributes. For information, see *Using Extensible Attributes*.

• **Permissions:** Define administrative permissions. For information, see *About Administrative Permissions*.

3. Click **Toggle Advanced Mode** if the editor is in basic mode. When the additional tabs appear, you can do the following in each tab:
  - **General:** Click the **Advanced** subtab and view the networks associated with the zone. This tab is visible only if the primary server is a Grid member, Microsoft server, or unassigned.
    - If a zone is associated with one or more networks, the IP addresses of its host, A and AAAA records must belong to the associated networks. You cannot change the network associations in this editor. Navigate to the DHCP Network editor of the network, to change the zone associations. For information, see *Associating Networks with Zones*.
  - **DNS Integrity Check:** Configure the appliance to monitor DNS data in the NS RRsets for authoritative zones. The appliance generates alerts when data discrepancies have been detected so you can mitigate possible DNS domain hijacking. For more information, see *About DNS Integrity Check for Authoritative Zones*.
  - **Host Naming:** Set restrictions for host names. For information, see *Specifying Hostname Policies*.
  - **Shared Record Groups:** Add shared record groups to a zone. For information, see *About Shared Record Groups*.
  - **DNSSEC:** Configure DNSSEC properties. For information, see *Chapter 22, DNSSEC*.
  - **Record Scavenging:** Define the rules for DNS records scavenging in the zone, as described in *Configuring DNS Record Scavenging Properties*.
  - **Updates:** Click the **Advanced** subtab and specify the secure dynamic updates settings, as described in *Secure Dynamic Updates*.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

or

Click the **Schedule icon** at the top of the wizard to schedule this task. In the **Schedule Change panel**, enter a date, time, and time zone. For information, see *Scheduling Tasks*.

### About DNS Integrity Check for Authoritative Zones

In certain DNS domain hijacking scenarios, hijackers alter the DNS data of a domain after gaining control of it. They consequently redirect users to a fraudulent site, instead of the legitimate site, on the Internet. To protect your authoritative DNS server against this type of DNS domain hijacking, you can configure the appliance to periodically monitor DNS data for top-level or parent authoritative zones. Based on your configuration, the appliance periodically checks DNS data in the NS RRsets for these zones and compares the data with that in the appliance database. It then reports data discrepancies through SNMP traps and logs related events in the syslog. You can also monitor the status of DNS data discrepancies, if any, through the **DNS Integrity Check** widget on the Task Dashboard. The severity in data discrepancies can help identify possible domain hijacking.

DNS integrity check is supported on all Infoblox appliances, including Advanced Appliances used primarily for Infoblox. For information about Infoblox, see *About Infoblox Advanced DNS Protection*. You can configure DNS integrity check for any selected authoritative zones, but you cannot configure it at the Grid, member, or DNS view level.

When you enable this feature, the appliance queries the NS RRsets and glue records for the top-level authoritative zones and compare the data with that in the appliance database. It does not query data for sub zones or delegated zones in the Grid.

### Configuring DNS Integrity Check

To configure the appliance to check NS and glue records for a top-level or parent authoritative domain, complete the following:

1. From the **Data Management** tab, select the **DNS** tab -> **Zones** tab -> top-level **authoritative zone** that you want to monitor, and then click the **Edit** icon from the Toolbar. Note that you can configure this feature only at the zone level. You can also configure zones that have the same name in different DNS views.

   **Note:** Once you configure a zone for DNS integrity check, you will not be able to add a parent zone above this zone. You must disable DNS integrity check for this zone before you can add the parent zone.

2. In the **Authoritative Zone** editor, toggle to the **Advanced Mode**, select the **DNS Integrity Check** tab -> **Basic** tab and complete the...
2. **Enable:** Select this check box to enable the DNS integrity check feature.

   **Member:** Click **Select Member** to select the Grid member you want to use for DNS integrity check. When you select a member, ensure that the member is configured to send and receive DNS queries and responses from Grid primaries (including stealth primaries) for the zone being monitored. Note that queries generated by DNS integrity check for the first reachable internal Grid primary (including a stealth primary) are logged in relevant DNS reports. For information about reports, see *Infoblox Reporting and Analytics.*

   **Check Frequency:** Enter how often the appliance monitors DNS data for the authoritative zone. Select the time unit from the drop down list. The appliance periodically queries DNS data for the top-level zone based on the time interval you configure here. The default value is one hour, and the minimum configurable value is 15 minutes.

   **Enable Verbose Logging:** Select this to enable detailed logging of events related to DNS integrity check. When you select this option, the appliance logs additional information in the syslog when DNS data discrepancies are detected. It also logs a message when no data discrepancies are found during a DNS data check. When you clear this check box, the appliance logs standard information in the syslog and does not log an event when no data discrepancies are found during a DNS integrity check. This is disabled by default. For information about the syslog, see *Viewing the Syslog.*

3. Save the configuration.

### Monitoring DNS Data Discrepancies for Authoritative Zones

When the appliance detects DNS data discrepancies between the authoritative and delegated zones, it reports the discrepancies through SNMP traps and email notifications, if configured. For more information, see *Setting SNMP and Email Notifications.* The appliance classifies data discrepancies by severity, as follows:

- **Critical:** Data in the NS RRsets for the authoritative and delegate zones are completely out of synchronization.
- **Severe:** Some data in the NS RRset between the authoritative and delegate zones overlaps and some data is different.
- **Warning:** The NS RRset for the authoritative zone is a subset of the NS RRset for the delegate zone. It is possible that incorrect IP addresses have been entered at the registrar.
- **Informational:** The NS RRset for the delegate zone is a subset of the NS RRset for the authoritative zone. This could indicate a possible delay in domain registration.
- **Normal:** There are no DNS data discrepancies between the NS RRsets for the authoritative and delegated zones.
- **None:** No DNS discrepancies data has been collected or DNS integrity check has not been performed.

When different Grid primaries report different severity levels for the same data check, the appliance reports the most severe discrepancy level. When different Grid primaries report the same severity for the data check, the appliance reports only the first check.

You can use the following methods to monitor DNS data discrepancies for selected authoritative zones:

- Viewing syslog events, as described in *Viewing the Syslog.*
- Monitoring DNS data discrepancy status through the *DNS Integrity Check* dashboard widget, as described in *DNS Integrity Check.*
- Receiving SNMP traps and email notifications, as described in *Setting SNMP and Email Notifications.*

### About Domains and Zones

After creating a zone, you can add more zones at the same level, or add subordinate zones (*subzones*). The subzones can be authoritative, delegated, forward, or stub.

The distinction between domains and zones is that domains provide a logical structure to the DNS name space while zones provide an administrative structure. The difference between domains and subdomains and zones and subzones is that the terms *subdomains* and *subzones* reference their relationship to a parent domain or zone. With the exception of the root domain and root zone, all domains are subdomains and all zones are subzones.

You can organize a domain based on logical divisions such as type (\.com,\.gov,.edu; or sales, eng, sup) or location (\.uk,\.jp,\.us; or hq, east, west). *Figure 19.1* shows one way to organize the external (public) name space and the internal (private) name space for a corporation with the domain name *corpxyz.com.* The external name space follows standard DNS conventions. Internally, you can create an individual subdomain and corresponding subzone for each department.

*Figure 19.2 Domains and Subdomains, and Forward-Mapping Zones and Subzones*
On the Infoblox appliance, you can configure and manage DNS zones and subzones.

**IDN Support For DNS Zones**

Grid Manager supports IDNs for DNS zones and resource records. For information about IDN, see [Support for Internationalized Domain Names](#). You can use either IDN or punycode (representation of IDN) to create DNS zones. Even if you use punycode to create a zone, the appliance automatically generates the corresponding IDN and displays the zone name in its native characters. Make sure that you use valid punycode to create a DNS zone. If you specify an invalid punycode, the appliance retains the punycode and does not convert it into IDN. Note that the appliance displays both the IDN and punycode for an IDN zone.

The following table summarizes how the appliance displays IDNs at the DNS zone level:

<table>
<thead>
<tr>
<th>Input</th>
<th>NIOS Displays...</th>
<th>NIOS DNS Domain (Punycode in the GUI)</th>
<th>Conversion Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello.com</td>
<td>hello.com</td>
<td>hello.com</td>
<td>No conversion</td>
</tr>
<tr>
<td>.com</td>
<td>.com</td>
<td>xn--80adk5aaihr3f9e.com</td>
<td>IDN to punycode</td>
</tr>
<tr>
<td>xn--80adk5aaihr3f9e.com.com</td>
<td>.com</td>
<td>xn--80adk5aaihr3f9e.com</td>
<td>Punycode to IDN</td>
</tr>
<tr>
<td>\xyz format</td>
<td>\xyz format</td>
<td>\xyz format</td>
<td>No conversion</td>
</tr>
</tbody>
</table>

**Assigning Zone Authority to Name Servers**

Forward-mapping zones answer name-to-address queries, and reverse-mapping zones answer address-to-name queries. When you create an authoritative forward-mapping zone or reverse-mapping zone, you assign zone authority to a name server and define it as the primary server for the zone. A primary server is designated as the primary source for the zone and maintains a master copy of the zone data. In a traditional DNS configuration, zone updates are performed based on a model that consists of a single primary server and one or multiple secondary servers, which receive read-only zone updates from the primary through database replications or zone transfers. Since the primary server contains editable zone data and is designated as the primary source for the zone, it can become a single point of failure when it becomes unavailable. To avoid a single point of failure for zone transfers, you can configure multiple primary servers for an authoritative zone. When you define multiple primary servers for a zone, each primary has a copy of the zone's authoritative data that can be updated independently. When you modify zone data, the appliance replicates updated data among all primary servers. When there are conflicts between zone updates, the appliance generally selects the latest updates based on the timestamps the updates were made by the clients to the primary servers. Therefore, accurate time synchronization among all servers in the DNS configuration is very important. For more information about other best practices for configuring multiple primaries for an authoritative zone, see [Best Practices for Defining Multiple Primaries for Authoritative Zones](#).

You can also create one or more secondary name servers for a zone. A secondary server for a zone receives read-only zone data from the primary server. If a zone is part of an internal DNS structure for a private network, the inclusion of a secondary DNS server is optional, though highly recommended. If a zone is part of an external DNS structure for a public network such as the Internet, then a secondary server in a different subnet from the primary server is required. This requirement provides an additional safeguard against localized network failures causing both primary and secondary name servers for a zone to become inaccessible.

**Note:** The primary/secondary relationship between name servers is also known as a master/slave relationship. You can enter, modify, and remove zone data on the primary (or master) servers, which can then send new and modified data in a read-only format to the secondary (or slave) servers. Both primary and secondary name servers are authoritative for the zone data they serve. The distinction between them is how they get their zone data.
In Grid Manager, you can specify the primary and secondary servers for a zone or you can specify a name server group. A name server group is a collection of one or more primary servers and one or more secondary servers. For information on name server groups, see About Name Server Groups.

Best Practices for Defining Multiple Primaries for Authoritative Zones

Before you configure multiple primary servers for a zone, consider the following guidelines to ensure data integrity:

- This feature is designed to increase availability of the DNS service by allowing multiple primaries for a zone. It will not increase overall throughput of DNS update traffic, as ultimately all updates must be replicated to (and processed by) all of the primaries.
- When determining which appliances should act as primaries for the zone, consider that an additional SOA record will be required in the database for each primary. This will add to the overall record count for the zone, and each SOA will need to be updated for any change to the zone, which can impact performance.
- Enable NTP for all members (at the member level) and ensure that their times are properly synchronized with their local time servers. Ensure that you select the "Exclude the Grid Master as an NTP server" option. The appliance selects the latest zone updates based on the timestamps the updates were made by clients to the primary servers. This is especially important when there are conflicts between two or more zone updates. For information about NTP, see Using NTP for Time Settings.
- When specifying the primary server for secondary zones, you can choose to have the appliance automatically select it for you based on latency determination or you can manually specify it. When manually selecting a primary for zone updates, consider using one that is close in proximity to the secondary servers, which can result in better service performance. For information about setting preference for the primary server, see Adding Grid Secondaries.
- You can configure a default primary for DDNS updates to a zone with multiple primary servers. To enhance service performance, select a default primary that is close in proximity to the DHCP server that provides DDNS updates. This is especially useful if you have DHCP members that are located in different locations. You can configure a different default primary for each DHCP member based on their locations. For more information, see Defining the Default Primary for DDNS Updates to Zones with Multiple Primaries.
- DNSSEC is not supported for zones with multiple primary servers. These zones must be unsigned. For information about DNSSEC, see About DNSSEC.
- When determining which appliances should act as primaries for the zone, consider that an additional SOA record will be required in the database for each primary. This will add to the overall record count for the zone, and each SOA will need to be updated for any change to the zone, which can impact performance.

Specifying a Primary Server

When you create a zone, the primary server can be a Grid member, an external DNS server that you specify, or a Microsoft DNS server that is managed by a Grid member. For information about managing Microsoft Windows DNS servers, see Chapter 34, Managing Microsoft Windows Servers.

Although a zone typically has only one primary server, you can specify multiple primary servers for an authoritative zone. You can configure multiple Grid primaries or multiple external primaries (including Microsoft AD-integrated servers) for a zone, but you cannot configure both at the same time for the same zone. In addition, you can configure one Microsoft server, but not multiple Microsoft servers (except for Microsoft AD-integrated servers), as the primary server for a zone. Note that each primary server that you configure for a zone has its own MNAME for the SOA record and serial number. For information about how to view and modify certain values in the SOA record, see Viewing and Modifying SOA Records.

A hidden primary provides data to its secondary servers, which in turn respond to DNS queries using this data. One of several advantages of this approach is that you can take the primary server offline for administrative or maintenance reasons without causing a disruption to DNS service (within the expiration interval set for the validity of its zone data—the default is 30 days).

When you add an authoritative forward-mapping zone and assign responsibility for the zone to a primary name server whose host name belongs to the same namespace of the zone, the NIOS appliance automatically generates an NS (name server) record and an A (address) record for the name server. This type of A record is called a glue record because it "glues" the NS record to the IP address (in the A record) of the name server.

In Grid Manager, you can specify the primary server for a zone when you create it using the Add Authoritative Zone wizard or when you edit an existing zone using the Authoritative Zone editor. For information on how to add a new zone through the wizard, see Configuring Authoritative Zones. The following procedure describes how to access the editor of a zone. To specify a primary server for an existing zone:

1. From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and then click the Edit icon.
2. In the Authoritative Zone editor, click Name Servers.
3. Select Use this set of name servers.
4. Click the Add icon and select one of the following options for a primary server:
   - Grid Primary: Choose this option to select a Grid member as the primary server for the zone. See Specifying Grid Primary Servers.
   - Microsoft Primary: Choose this option to select a Microsoft DNS server as the primary server for the zone. See Specifying Microsoft Primary Servers.
   - External Primary: Choose this option if the appliance is in a Grid and you want to specify a primary server outside the Grid ("external" to the Grid). See Specifying External Primary Servers.
5. Save the configuration and click Restart if it appears at the top of the screen.

Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

Specifying Grid Primary Servers

In the Add Grid Primary panel, do the following, and then click Add to add the Grid member to the list of name servers for the zone as primary:
• If no member is displayed, click Select to specify a Grid member. When there are multiple members, Grid Manager displays the Member Selector dialog box from which you can select a primary name server. To select multiple primary servers, click Select and then Add again.

• Stealth: Click this to hide the NS record for the primary name server from DNS queries. The NIOS appliance does not create an NS record for the primary name server in the zone data. Clear the check box to display the NS record for the primary name server in responses to queries.

Changing the SOA Name for a Zone

If the primary name server of a zone is a Grid member, the NIOS appliance allows you to change the SOA (start of authority) name that is automatically created when you initially configure the zone. For example, you might want to hide the primary server for a zone. If your appliance is named dns1.zone.tld, and for security reasons, you may want to show a secondary server called dns2.zone.tld as the primary server. To do so, you would go to dns1.zone.tld zone (being the true primary) and change the SOA to dns2.zone.tld to hide the true identity of the real primary server.

To change the SOA name for a zone:

1. From the Data Management tab, select the DNS tab > Zones tab > dns_view -> zone check box -> Edit icon.
2. In the Authoritative Zone editor, click Settings.
3. Click Override beside the Primary name server field and enter the new SOA name. This field supports IDN.
4. Save the configuration and click Restart if it appears at the top of the screen.
   or
   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

Specifying Microsoft Primary Servers

You can assign a Microsoft server as the primary server of a zone when it is managed by a Grid member in read/write mode. For information, see Chapter 34, Managing Microsoft Windows Servers. When a Microsoft server is the primary server of a zone, the zone supports only standard DNS resource records. It does not support the Infoblox record types host records, bulk host records, and shared record groups. You cannot add any of these records to the zone nor assign a DNS zone with these records to a Microsoft server as the primary server.

In the Add Grid Primary panel, do the following to assign a Microsoft primary server:

1. Complete the following:
   • Select Use this set of name servers.
   • Click the Add icon and select Microsoft Primary.
2. In the Add Microsoft Primary panel, do the following, and then click Add to add the Microsoft primary server to the list of name servers for the zone:
   • If no server is displayed, click Select Server to specify a Microsoft server. When there are multiple servers, Grid Manager displays the Server Selector dialog box from which you can select a Microsoft server. Grid Manager lists Microsoft servers that are managed in read/write mode. It does not include Microsoft servers managed in read-only mode.
   • Information to create NS record: Grid Manager automatically creates the NS record. After you select a server, Grid Manager populates the Name and IP Address fields. Grid Manager uses this information when it creates the NS record, unless you select Stealth. You can specify a different FQDN or IP address for the NS record; for example, for a multihomed server.
   • Store the zone in Active Directory (AD Integrated Zone): This is enabled and selected by default only if the Microsoft server is a domain controller. Note that you can enable Active Directory integration only after the Microsoft server has been synchronized at least once because its AD ability is not known before the synchronization. This is disabled when the Microsoft server is not a domain controller.
   • Stealth: Select this option to hide the NS record for the primary name server from DNS queries. Grid Manager does not create an NS record for the primary name server in the zone data. Clear this option to display the NS record for the primary name server in responses to queries. Note that this option is not available for AD-integrated zones.

Specifying External Primary Servers

In the Add External Primary panel, do the following, and then click Add to add the external primary server to the list of name servers for the zone:

• Name: Type a resolvable domain name for the external primary server.
• Address: Type the IP address of the external primary server.
• Multi-master: This appears only when there is more than one external primary assigned to the zone. Select this check box for external primary servers when the zone is in another Grid and has multiple Grid primaries. When you select this option, it is selected for all external primaries assigned to the zone. This zone is identified as an external zone with multiple primary servers.
• Use TSIG: To authenticate zone transfers between the local appliance and the external primary server using a TSIG (transaction signature), select this check box. Infoblox TSIGs use HMAC-MD5 hashes. These are keyed one-way hashes for message authentication codes using the Message Digest 5 algorithm. For details, see RFC 1321, The MD5 Message-Digest Algorithm, and RFC 2104, HMAC: Keyed-Hashing for Message Authentication.
• Key name: Type or paste the name of the TSIG key you want to use. This must be the same name as that of the TSIG key on the external primary server.
• Key Data: Type or paste a previously generated key. This key must also be present on the external primary server. You can generate a TSIG key, or obtain the TSIG key name and key from the external name server, by accessing the server yourself or by requesting the server administrator to deliver them to you through some out-of-band mechanism. Then type or copy-and-paste the name and key into
the appropriate fields.

- **Use 2.x TSIG:** If you want to use TSIG authentication and the external primary name server is a NIOS appliance running DNS One 2.x code, select this check box. The local appliance generates the required TSIG key for authenticating DNS messages to and from appliances running DNS One 2.x code.

**Note:** On the appliance you configure as a secondary server for a zone, you must associate a TSIG key for each primary server to which the secondary server requests zone transfers. On the appliance you configure as a primary server for a zone, you can set a TSIG key at the Grid, member, or zone level. Because the secondary server requests zone transfers, it must send a specific key in its requests to the primary server. Because the primary server responds to the requests, it can have a set of TSIG keys from which it can draw when responding. As long as the primary server can find the same TSIG key that the secondary sends it, it can verify the authenticity of the requests it receives and authenticate the responses it sends. Use NTP to synchronize the time on both name servers that use TSIG-authenticated zone transfers.

### Specifying Secondary Servers

A secondary name server is as authoritative for a zone as a primary server. Like a primary server, a secondary server answers queries from resolvers and other name servers. The main difference between a secondary and primary server is that a secondary server receives all its data from a primary server, or possibly from another secondary server that relays zone data it receives. The zone data passes from a primary to a secondary server (and possibly from that secondary server on to another secondary server). This process is called a zone transfer.

The advantage of using primary and secondary name servers is that you enter and maintain zone data in one place—on the primary server. The data is then distributed to the one or more secondary servers.

Secondary servers can be Grid members, external DNS servers or Microsoft DNS servers that are managed by Grid members. In Grid Manager, you can specify the secondary server for a zone when you create it using the Add Authoritative Zone wizard and when you edit an existing zone using the Authoritative Zone editor. For information on how to add a new zone through the wizard, see Configuring Authoritative Zones. The following procedure describes how to specify the editor of a zone.

To specify a secondary server for an existing zone:

1. From the Data Management tab -> DNS tab -> Zones tab -> zone check box, and then click the Edit icon.
2. In the Authoritative Zone editor, click Name Servers.
3. Select Use this set of name servers.
4. Click the Add icon and select one of the following options:
   - **Grid Secondary:** Selects the local appliance as the secondary server (or if the appliance is deployed in a Grid and you want to make a different member the secondary server). See Adding Grid Secondaries.
   - **Microsoft Secondary:** Select this option if you want to specify a managed Microsoft DNS server as a secondary server. See Specifying Microsoft Secondary Servers.
   - **External Secondary:** Select this option if you want to specify a secondary server outside the Grid (“external” to the Grid), or if the appliance is deployed independently from a Grid. See Specifying External Secondaries.
5. Save the configuration and click Restart if it appears at the top of the screen. or

Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

### Adding Grid Secondaries

When adding Grid secondaries to a zone that has multiple primary servers, the appliance selects a primary server as the active server based on the method that you have selected. If you select Automatic, the primary is selected based on latency determination, which occurs separately on each primary. When available, the primary server that has the lowest latency is preferred. When you select Manual, latency determination is ignored, and the first available primary server in the list is selected as the active server. Thus if the first primary on the list is not available, the next available primary is used. Depending on which primary server is selected, the Grid secondary returns the FQDN of the primary in the MNAME field of the zone SOA record. It also includes the version of the zone content that it serves.

In the Add Grid Secondary panel, enter the following, and then click Add to add the Grid secondary server to the list of name servers for the zone:

- If no member is displayed, click Select to specify a Grid member. When there are multiple members, Grid Manager displays the Member Selector dialog box from which you can select a secondary name server.
- **Stealth:** This setting applies only if the primary server is a Grid member or Microsoft server. Select this to hide the NS record for the secondary name server from DNS queries. The NIOS appliance does not create an NS record for this name server in the zone data. Select the check box again to display the NS record for the secondary name server in responses to queries. A secondary server in stealth mode is also known as a “hidden secondary”.
  
  For example, you can configure a hidden secondary when a secondary server is at a branch office with a slow connection to the rest of corporate network. Configure local hosts at the branch office to send DNS queries to the secondary server, but keep it hidden from other name servers on the rest of the network so that they do not send it queries. Instead, they use a server located in a different part of the network that has faster connection speeds.
- **Lead Secondary:** This option becomes available only after you specify the primary name server as external. When a primary server is external to a Grid whose members are secondary servers, you can select this check box to designate one member as a lead secondary. The primary server sends zone transfers to the lead secondary, which distributes the zone data to the other secondary servers in the Grid using zone transfers (not the Grid data replication mechanism). After you designate a Grid member as a lead secondary for a zone, you do not have to configure members to use the lead secondary server. All other Grid members acting as secondary servers for the zone automatically use the lead secondary to get zone data. Using a lead secondary simplifies the addition, modification, and removal of other secondary servers in the Grid. As long as the lead secondary remains unchanged, you need not update intervening firewall policies or the external primary server whenever you make changes to non-lead secondary Grid members. This approach also reduces the amount of traffic between primary and secondary servers.
- **Update Zones Using:** This option becomes available only after you specify a Grid member as the primary server.
### Specifying Microsoft Secondary Servers

You can assign a Microsoft server as the primary server of a zone when it is managed by a Grid member in read/write mode. For information, see Chapter 34, Managing Microsoft Windows Servers.

Since Microsoft servers cannot replicate data from the Grid, when a DNS zone is defined as a secondary on a Microsoft server, the Microsoft server obtains the content of the zone only through DNS zone transfers.

- In the Add Microsoft Secondary panel, do the following:
  - If no server is displayed, click Select Server to specify a Microsoft server. When there are multiple servers, Grid Manager displays the Server Selector dialog box from which you can select a Microsoft server. Grid Manager lists Microsoft servers that are managed in read/write mode. It does not include Microsoft servers managed in read-only mode.
  - Information to create NS record: Grid Manager automatically creates the NS record. After you select a server, Grid Manager populates the Name and IP Address fields. Grid Manager uses this information when it creates the NS record, unless you select Stealth.
  - Stealth: This setting applies only if the primary server is a Grid member or a Microsoft server. Select this option to hide the NS record for the secondary name server from DNS queries. Grid Manager does not create an NS record for this name server in the zone data. Clear this option to display the NS record for the secondary name server in responses to queries.

### Specifying External Secondaries

In the Add External Secondary panel, enter the following, and then click Add to add the external secondary server to the list of name servers for the zone:

- **Name**: Enter a resolvable domain name for the external secondary server.
- **Address**: Enter the IP address of the external secondary server.
- **Stealth**: This setting applies only if the primary server is a Grid member or a Microsoft server. Click this check box to hide the NS record for the secondary name server from DNS queries. The NIOS appliance does not create an NS record for the secondary name server in the zone data. Select the check box again to display the NS record for the secondary name server in response to queries.

**Note**: To avoid an impact on your database performance, Infoblox recommends that you do not configure a large number of external secondary servers in stealth mode. To ensure that these secondary servers receive notifications about zone updates, you can allow zone transfers for these IP addresses and then enable the appliance to add them to the also-notify statement. For information about how to configure this feature, see Configuring Zone Transfers.

- **Use TSIG**: To authenticate zone transfers between the local appliance and the external secondary server using a TSIG (transaction signature), select this check box. Infoblox TSIGs use HMAC-MD5 hashes. These are keyed one-way hashes for message authentication codes using the Message Digest 5 algorithm. For details, see RFC 1321, The MD5 Message-Digest Algorithm, and RFC 2104, HMAC: Ke yed-Hashing for Message Authentication.
- **Key name**: Type or paste the name of the TSIG key you want to use. This must be the same name as that of the TSIG key for this zone on the external secondary server.
- **Key**: Type or paste a previously generated key. On the external secondary server, this key must also be present and associated with this zone. You can generate a TSIG key, or you can obtain the TSIG key name and key from the external name server, either by accessing the appliance yourself or by requesting the appliance administrator to deliver them to you through some out-of-band mechanism. Then, type or copy-and-paste the name and key into the appropriate fields.
- **Use 2.x TSIG**: Select this check box to use TSIG authentication and the external secondary name server is a NIOS appliance running DNS One 2.x code. The local appliance generates the required TSIG key for authenticating DNS messages to and from appliances running DNS One 2.x code.

**Note**: On the appliance you configure as a secondary server for a zone, you must associate a TSIG key for each primary server to which the secondary server requests zone transfers. On the appliance you configure as a primary server for a zone, you can set a TSIG key at the Grid member, or zone level. Because the secondary server requests zone transfers, it must send a specific key in its requests to the primary server. Because the primary server responds to the requests, it can have a set of TSIG keys from which it can draw when responding. As long as the primary server can find the same TSIG key that the secondary sends it, it can verify the authenticity of the requests it receives and authenticate the responses it sends. Use NTP to synchronize the time on both name servers that use TSIG-authenticated zone transfers.
Configuring Domain Controller List

When you configure an AD-integrated authoritative zone, by default all the domain controllers that belong to the domain automatically add NS records to the AD-integrated zone, which might be undesirable in some deployment scenarios. For example, if a domain controller is deployed in a company's branch office, it is unlikely that the domain controller should be registered as the name server for the company's top-level zones. By configuring a domain controller list for the AD-integrated zone, you can control which domain controllers are allowed to add NS records to the zone. If you configure a domain controller list for an AD-integrated zone, only those in the list can add NS records to the zone. You can configure the domain controller list for AD-integrated zones either on the NIOS appliance or on the Microsoft server.

Configuring Domain Controller List on NIOS

You can configure a domain controller list for an AD-integrated authoritative zone to allow NS record creation for specific domain controllers. You can add, modify, and delete the entries in the domain controller list if the Microsoft server assigned to the zone is managed in read/write mode. If you have not configured the domain controller list while configuring an AD-integrated zone, you can perform the configuration later while editing the zone.

Note the following about the domain controller list:

- If the domain controller list is empty for an AD-integrated zone, all domain controllers that belong to the domain can add NS records to the AD-integrated zone.
- If you remove a domain controller from the domain controller list of an AD-integrated zone, the NS record that belongs to the domain controller is not automatically deleted. You must manually delete the NS record from the AD-integrated zone.

To configure a domain controller list for an AD-integrated zone:

1. From the Data Management tab, select the DNS tab -> Zones tab -> click the Add icon and select Authoritative Zone from the drop-down menu.
2. Complete the details as mentioned in Configuring Authoritative Zones and then complete the following to specify a list of domain controllers that are allowed to add NS records to the AD-integrated zone:
   - **No**: Select No if you do not want to configure a domain controller list for the AD-integrated zone. If you select No, all domain controllers that belong to the domain can add NS records to the AD-integrated zone.
   - **Yes**: Select Yes to configure a domain controller list for the AD-integrated zone.
     - If you select Yes, click the Add icon of the Domain Controller table and select one of the following from the drop-down menu:
       - **Add**: Select this to manually add the IP addresses of the domain controllers to the list. Grid Manager adds a new row to the table. Specify the following:
         - **Address**: Enter the IP address of the domain controller.
         - **Comment**: Enter information about the domain controller.
     - **Auto-populate**: Select this to automatically populate the Domain Controller table with the list of domain controllers. In the Add Prepopulated Domain Controllers panel, select one of the following options:
       - **Zone**: Select this to copy the list of domain controllers from an existing AD-integrated zone in the NIOS database. Click Select to select the AD-integrated zone. Click Clear to remove the selected zone.
       - **Servers in Domain**: Select this to add the IP addresses of all the Microsoft servers available in the NIOS database which belong to the same AD domain as the primary Microsoft server assigned to the zone.
       - **Click Add** to add the list of domain controllers to the table. Grid Manager automatically populates the Domain Controller table with the list of domain controllers in ascending order by IP address.

   **Note**: The Auto-populate option to add the domain controller list is only available while configuring the AD-integrated zone. It is not available when you edit the domain controller list in the Authoritative Zone editor.

3. Save the configuration.

Configuring Domain Controller List on the Microsoft Server

You can configure a list of domain controllers that are allowed to add NS records to an AD-integrated zone on the Microsoft server using the dnscmd command line utility as follows:

dnscmd DNS Server /Config Zone Name /AllowNSRecordsAutoCreation Ip Addresses

For example, if you are configuring a domain controller list for an AD-integrated zone foo.net on the DNS server, 192.69.0.1, use the following command:

dnscmd 192.69.0.1 /config foo.net /AllowNSRecordsAutoCreation 192.69.0.6 192.69.0.9

For more information about configuring a domain controller list for an AD-integrated zone on the Microsoft server see https://technet.microsoft.com/en-us/library/cc755848%28v=ws.10%29.aspx.

Importing Zone Data

Importing zone information alleviates having to manually enter data through the Infoblox GUI. You can import data from existing name servers, as well as from NIOS appliances running version 3.1r4 or later. You can import existing zone data when you create a new zone and when you edit an existing zone. You can import one zone (and its subzones) at a time.

For the remainder of this section, the name server that stores the existing zone data (which is imported) is referred to as the **source** name server (regardless of whether it is a third-party server or another NIOS appliance). The appliance that receives the zone data is referred to as the **destina**
The appliance imports zone data through a zone transfer. Therefore, the source name server must be authoritative for the zone data being imported. You must also configure the source name server to allow zone transfers to the destination appliance. On the source name server, you might need to modify the `allow-transfer` substatement to include the IP address of the destination appliance prior to importing the data. If you are importing zone data to an HA pair, use the VIP (virtual IP) address shared by the HA pair. For a single independent appliance, use the LAN IP address. If you are importing zone data to a Grid, always use the IP address of the Grid Master.

If the source name server is an Infoblox appliance, you can configure it to allow zone transfers as described in [Enabling Zone Transfers](#). Note that a NIOS appliance, acting as the primary name server for a zone, by default allows zone transfers to its secondary name servers. If the zone import fails, the zone to which the data is imported will be disabled and the system does not create records and delegated subzones.

**Note:** The appliance does not encode punycode when you import zone data containing punycode. For example, a zone data containing IDNs in punycode is stored in punycode for the data being imported. The data is managed in punycode only.

### About Importing Data into a New Zone
When the appliance imports data to a newly created zone, it imports the existing A, CNAME, DNAME, SRV, TXT, MX, PTR, host, and bulk host records, but creates NS (and A records matching that NS record) and SOA records appropriate for the destination server. The NS and SOA records are auto-created when a destination appliance is specified as the primary or secondary name server for the new zone. If the imported zone has extra NS records, they are rewritten to specify the source server as an external secondary. Delegation is also added for any subzones. The subzone records are not imported.

### About Importing Data into an Existing Zone
When you import zone data into an existing zone, the zone retains the NS and SOA records automatically created when the zone was originally...
created and replaces all other records—A, PTR, MX, TXT, SRV, CNAME, DNAME, host, and bulk host. The local appliance also retains subzones and records in the subzones that exist locally. If there are no duplicates, the destination appliance records are retained. If the imported zone has extra NS records, those records change to designate the source server as an external secondary.

Importing Data into Zones

In Grid Manager, you can import zone data when you create the zone using the Add Authoritative Zone wizard and when you edit an existing zone. For information on how to add a new zone through the wizard, see Configuring Authoritative Zones. The last step of the wizard provides the option to import zone data. The following procedure describes how to import data into an existing zone.

Note: Only superusers can import zone data that contains A, AAAA, shared A, or shared AAAA records with a blank name. Limited-access users must have read/write permission to Adding a blank A/AAAA record in order to import zone data that contains A, AAAA, shared A, or shared AAAA records with a blank name, otherwise the import zone data operation might fail. You can assign global permission for specific admin groups and roles to allow to import A, AAAA, shared A, or shared AAAA records with a blank name. For more information, see Administrative Permission s for Adding Blank A or AAAA Records.

To import data into an existing zone:

1. From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and then click Import Zone in the Toolbar.
2. In the Import Zone dialog box, specify the following:
   - The IP address of the name server from which you want to import data.
   - Optionally, click the Automatically create Infoblox host records from A records check box.
3. Click Import.

When the local server successfully imports the zone data, a Confirmation message appears. If the local server cannot import the zone data, an Error message appears, recommending that you verify the correctness of the IP address of the remote server and zone information.

Note: If NIOS resolves the IP address of the imported zone data, an external secondary member is added to the list of name servers with the exact IP address. If NIOS cannot resolve the IP address of the imported zone data, it adds an external secondary member with the IP address 255.255.255.255 to the list of name servers.

Removing Zones

Depending on the configuration, you may or may not be able to delete or schedule the deletion of a zone and all its contents. Superusers can determine which group of users are allowed to delete or schedule the deletion of a zone and all its contents. For information about how to configure the recursive deletion of zones, see Configuring Recursive Deletions of Networks and Zones.

Note that you must have Read/Write permission to all the subzones and resource records in order to delete a zone. The possible effects of removing or re-parenting are illustrated in Figure 19.4. The appliance puts all deleted objects in the Recycle Bin, if enabled. You can restore the objects if necessary. When you restore a parent object from the Recycle Bin, all its contents, if any, are re-parented to the restored parent object. For information about the Recycle Bin, see Using the Recycle Bin.

Figure 19.4 Removing or Reparenting Subzones

Remove Zone B and ... or ... remove its subzones. or ... reparent its subzones.

The NIOS appliance removes zone B, subzone C, and all their resource records.

The NIOS appliance removes zone B and its resource records. It reparents subzone C to zone A, it creates a new NS record in zone A for subzone C and possibly changes admin privileges for subzone C.
If you choose to reparent the subzones, be aware of the following caveats and possible effects of the reparenting:

- You cannot remove a zone and reparent its subzones if at least one of the subzones is a delegated zone. You must first remove any delegated subzones, and then you can remove the zone and reparent its subzones.
- If there are AD (Active Directory) subzones (_msdcs, _sites, _tcp, _udp, domain dns zones, forest dns zones) and you opt to remove the parent zone only, the NIOS appliance reparents all subzones except the AD subzones, which it removes regardless of the removal option you specify.
- The subzone reparenting option is unavailable when you select multiple zones for removal.
- A record created under a top-level reverse-mapping zone is reparented when its immediate parent zone is created. If that parent zone is deleted, the record is restored to the top-level reverse-mapping zone.

Examples:

Example 1:
Step 1 - Add 10.in-addr.arpa under . (root zone)
Step 2 - If you add 10.in-addr.arpa, it is created under . (root zone)
Step 3 - If you add in-addr.arpa, then 10.in-addr.arpa is reparented under in-addr.arpa

Example 2
- Deleting in-addr.arpa from the hierarchy might lead to 10.in-addr.arpa reparenting under . (root zone), depending on the Remove zone only/ Remove all subzones option you select.
- If in-addr.arpa is restored, it is restored under . (root) zone with all its resource records.

Example 3
- Consider in-addr.arpa zone having 10.10.in-addr.arpa + 10.0.0.1 (PTR record)
- If you add 10.in-addr.arpa, then 10.10.in-addr.arpa is reparented under 10.in-addr.arpa
- and 10.0.0.1 PTR record is reparented from in-addr.arpa to 10.in-addr.arpa.
- If you delete 10.in-addr.arpa, then 10.10.in-addr.arpa is reparented under in-addr.arpa (depending on the Remove zone only / Remove all subzones option) and 10.0.0.1 PTR record is deleted along with 10.in-addr.arpa zone.
- When you remove a zone and reparent its subzones, any subzone that inherited its admin access settings from its previous parent zone (as opposed to having specific access settings for the subzone) now receive their settings from its new parent zone, which might be different. See Figure 19.5.5

Figure 19.5 Changed Admin Access Settings after Reparenting Subzones
Remove Zone B and ... ... reparent its subzones.

Before you remove zone B, subzone C inherits a “Deny” admin access setting from zone B.
After the removal, subzone C inherits “Read/Write” access from its new parent zone, zone A.

Note that if you set a specific “Deny” admin access privilege for subzone C before removing its parent zone (zone B), subzone C retains its specified “Deny” setting.

... the admin access settings for subzone C change because the privileges for its new parent zone (zone A) are different from those of its previous parent zone (zone B).

To remove a zone:

1. From the Data Management tab, select the DNS tab -> Zones tab.
2. Click the check box of the zones you want to delete.
3. Click the Delete icon.
4. Select one of the following. Note that these options appear only if you are allowed to delete zones and all its contents. For information about how to configure this, see Configuring Recursive Deletions of Networks and Zones.
   - **Remove zone only**: Select this to remove the zone and all its content. The appliance reparents all subzones to the parent zone of the zone that you want to remove, except for the automatically created AD (Active Directory) subzones.
   - **Remove all subzones**: Select this to remove the selected zone, all its subzones, and all the resource records of the selected zone and its subzones.
5. Click Yes.

You can also schedule the deletion for a later time. Click Schedule Deletion and in the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Deletions. For information about scheduling recursive deletions of zones, see Scheduling Recursive Deletions of Network Containers and Zones.

Restoring Zone Data

After you import or delete a zone, if you want the original zone back, you can restore it using the Recycle Bin. When you import a zone for the first time, the appliance saves the zone and its resource records as a single object in the Recycle Bin. It keeps the subzones with the zone. See Resto
When you reimport data into a zone, the software saves the zones, its resource records, and the delegated subzones created by the previous import operation in the Recycle Bin. It keeps the subzones (not created during the zone import) with the zone. See **Restoring Zone Data After a Zone Import Example**

If the zone import succeeds, the system adds resource records from the source to the target zone. It also adds delegated subzones for the source subzones. If the zone import fails, the system does not create records and delegated subzones. In either case, you can retrieve the original zone and its subzones from the Recycle Bin as follows:

- Delete the zone using the steps described in the section Removing Zones.
- Select **Remove zone only** to remove the zone and its resource records. The NIOS appliance reparents all subzones to the parent zone of the zone that you remove. Do not select **Remove all subzones**.
- Automatically created AD (Active Directory) subzones are an exception. Even if you select **Remove zone only**, the NIOS appliance still removes AD subzones.
- In the Finder panel, click **Recycle Bin**.
- Select the zone you want to restore and click the Restore icon.

The zone is restored back to its original state. The resource records are reparented back under it.

**Restoring Zone Data After a Zone Import Example**

In the example shown in **Figure 19.6**:

1. Import data from a source zone with subzones Sub x and Sub y into zone B with subzones Sub B1 and Sub B2. The appliance stores zone B and its resource records in the Recycle Bin.
2. To retrieve zone B after the import:
   - Delete subzone B using the **Remove zone only** option.
   - The appliance reparents subzones Sub B1 and Sub B2 to the Zone A, which is the zone above Zone B.
3. After the import, you can restore zone B from the Recycle Bin. The appliance reparents the subzones Sub B1 and Sub B2 back to zone B.

**Figure 19.6 Restoring Zones After a Zone Import**

**Restoring Zone Data After a Zone Reimport Example**

In the example shown in **Figure 19.7**:

1. You reimport data from the source zone with subzones Sub x and Sub y into zone B with subzones Sub B1 and Sub B2. To retrieve zone B after the import:
2. Delete the delegated subzones x and y and then remove subzone B using the **Remove zone only** option. The appliance stores zone B and its resource records and the previously-imported subzones Sub x and Sub y (as delegated subzones) in the Recycle Bin. It reparents subzones Sub B1 and Sub B2 to the zone above zone B (Zone A).
3. After the import, you can restore zone B and the subzones Sub x and Sub y from the Recycle Bin. The appliance reparents the subzones Sub B1 and Sub B2 back to zone B.

**Figure 19.7 Restoring Zones After a Zone Reimport**

Copyright ©2019, Infoblox, Inc. All right reserved.
Configuring Delegated, Forward, and Stub Zones

In addition to authoritative zones, the NIOS appliance allows you to configure delegated, forward, and stub zones. A delegated zone is a zone managed by (delegated to) another name server who owns the authority for the zone. A forward zone is where queries are sent before being forwarded to other remote name servers. A stub zone contains records that identify the authoritative name servers in another zone. This section covers the following topics:

- Configuring a Delegation
- Configuring a Forward Zone
- Configuring Stub Zones

Configuring a Delegation

Instead of a local name server, remote name servers (which the local server knows) maintain delegated zone data. When the local name server receives a query for a delegated zone, it either responds with the NS record for the delegated zone server (if recursion is disabled on the local server) or it queries the delegated zone server on behalf of the resolver (if recursion is enabled).

For example, there is a remote office with its own name servers, and you want it to manage its own local data. On the name server at the main corporate office, define the remote office zone as delegated, and then specify the remote office name servers as authorities for the zone.

You can delegate a zone to one or more remote name servers, which are typically the authoritative primary and secondary servers for the zone. If recursion is enabled on the local name server, it queries multiple delegated name servers based on their round-trip times. You can also add arpa as a top-level forward-mapping zone and delegate its subzones.

You can also configure TTL settings of auto-generated NS records and glue A and AAAA records for delegated zones in forward-mapping, IPv4 reverse-mapping, and IPv6 reverse-mapping zones. For information, see About Time To Live Settings.

The delegation must exist within an authoritative zone with a Grid primary server.

Configuring a Delegation for a Forward-Mapping Zone

To create a delegation for a forward-mapping zone:

1. From the Data Management tab, select the DNS tab -> Zones tab.
2. Click the parent zone to open it.
   Grid Manager displays the Records and Subzones tabs of the zone.
3. From the Subzones tab, click the Add icon -> Zone -> Add Delegation.
4. In the Add Delegation wizard, specify the following:
   - **Name**: This field displays a dot followed by the domain name of the current zone. Enter one or more labels before the dot to specify the domain name of the subzone.
   - **DNS View**: This field displays only when there is more than one DNS view in the network view. Displays the DNS view of the current zone.
   - **Comment**: Optionally, enter additional text about the zone.
   - **Lock**: This check box to temporarily disable this zone. For information, see Enabling and Disabling Zones
   - **Comment**: Optionally, enter additional text about the zone.

5. Click Next to assign a delegation name server group or define the name servers for the zone. Select one of the following:
- **UseThisNameservergroup**: Select this to assign a delegation NS group for the delegated zone. You can select the delegation NS group from the drop-down list.
- **UseThisSetOfNameservers**: Select this to define name servers for the delegated zone. In the Name Servers panel, click the Add icon and specify the following information:
  - **Name**: Enter the name of a remote name server to which you want the local server to redirect queries for zone data. This is a name server that is authoritative for the delegated zone.
  - **Address**: Enter the IP address of the delegated server.

For information about delegation NS group, see [Using Delegation Name Server Groups](#).

6. Save the configuration and click **Restart** if it appears at the top of the screen, or click **Next** to define extensible attributes as described in [Using Extensible Attributes](#).

   or

   Click the Schedule icon at the top of the wizard to schedule this task. In the ScheduleChange panel, enter a date, time, and time zone. For information, see [Scheduling Tasks](#).

---

**Note**
The DNS server resolves the FQDN of the delegated name server and does not use the IP address that you specify when assigning the delegated name servers.

### Configuring a Delegation for a Reverse-Mapping Zone

To create a delegation for a reverse-mapping zone:

1. From the DataManagement tab, select the DNS tab -> Zones tab.
2. Click the parent zone to open it.
   - Grid Manager displays the Records and Subzones tabs of the zone.
3. From the Subzones tab, click the Add icon -> Zone -> AddDelegation.
4. In the AddDelegation wizard, specify the following:
   - **IPv4Network**: This field displays if you are creating a delegation zone for an IPv4 reverse-mapping zone. Enter the IPv4 address for the address space for which you want to define the reverse-mapping zone and select a netmask from the Netmask drop-down list. Alternatively, you can specify the address in CIDR format, such as 192/8.
   - **IPv6NetworkPrefix**: This field displays if you are creating a delegation zone for an IPv6 reverse-mapping zone. Enter the IPv6 prefix for the address space for which you want to define the reverse-mapping zone and select the prefix length from the drop-down list.
   - **Name**: This field displays a dot followed by the domain name of the current zone. Enter one or more labels before the dot to specify the domain name of the subzone.
   - **DNS View**: This field displays only when there is more than one DNS view in the network view. Select a DNS view from the drop-down list.
   - **Comment**: Optionally, enter additional text about the zone.
   - **Disable**: Select this option to temporarily disable this zone.
   - **Lock**: Select this option to lock the zone so that you can make changes to it and prevent others from making conflicting changes.

5. Click **Next** to assign a delegation name server group or define the name servers for the zone. Select one of the following:
   - **UseThisNameservergroup**: Select this to assign a delegation NS group for the delegated zone. You can select the delegation NS group from the drop-down list.
   - **UseThisSetOfNameservers**: Select this to define name servers for the delegated zone. In the Name Servers panel, click the Add icon and specify the following information:
     - **Name**: Enter the name of a remote name server to which you want the local server to redirect queries for zone data. This is a name server that is authoritative for the delegated zone.
     - **Address**: Enter the IP address of the delegated server.

For information about delegation NS groups, see [Using Delegation Name Server Groups](#).

6. Save the configuration and click **Restart** if it appears at the top of the screen, or click **Next** to define extensible attributes as described in [Using Extensible Attributes](#).

   or

   Click the Schedule icon at the top of the wizard to schedule this task. In the ScheduleChange panel, enter a date, time, and time zone. For information, see [Scheduling Tasks](#).

---

**Note**
The DNS server resolves the FQDN of the delegated name server and does not use the IP address that you specify when assigning the delegated name servers.
Configuring a Forward Zone

When you want to forward queries for data in a particular zone, define the zone as a forward zone and specify one or more name servers that can resolve queries for the zone. You can also assign one or more external name servers as default forwarders for a forward zone. For example, define a forward zone so that the NIOS appliance forwards queries about a partner's internal site to a name server, which the partner hosts, configured just for other partners to access.

You can override the default forwarders for a forward-mapping zone at a Grid member level and configure custom forwarders. In other words, each Grid member can have its own forwarders for the forward zone. For example: a forward-mapping zone foo.com served by two Grid members M1 and M2 with M1 forwarding queries to 10.1.0.1 and 10.1.0.2 and M2 forwarding queries to 90.3.3.3 and 90.4.4.1. Note that the Grid member uses the default forwarders unless you override them at any level. For more information about domains and zones, see Configuring Authoritative Zone Properties.

Note: The use of a forward zone is different from that of a forwarder. (A forwarder is a name server that performs recursive lookups on behalf of the name servers that forward queries to it. For more information, see Using Forwarders.) A NIOS appliance forwards queries to the name server of a forward zone because the name server can resolve queries for the zone. A NIOS appliance forwards queries to a forwarder regardless of zones.

Note that a name server can have only one definition for a zone in any given DNS view; a forward zone cannot be configured on a member that already has a zone with the same domain name configured on it in the same DNS view. To configure a forward-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Forward Zone.
2. In the Add Forward Zone wizard, click Add a forward forward-mapping zone and click Next.
3. Enter the following information, and then click Next:
   - Name: Enter the domain name of the zone for which you want the NIOS appliance to forward queries.
   - DNS View: This field displays only when there is more than one DNS view in the current network view. Select the DNS view of the forward zone.
   - Comment: Enter a descriptive comment.
   - Disable: Click this check box to temporarily disable this zone.
   - Lock: Click this check box to lock the zone so that you can make changes to it and prevent others from making conflicting changes.
4. Click Next to assign a forward/stub server name server group or define the default zone forwarders to which the NIOS appliance forwards queries for the zone. Select one of the following:
   - Select Use this name server group to assign a forward/stub server NS group for the zone. You can select the forward/stub server NS group from the drop-down list. For information about forward/stub server NS groups, see Using Forward/Stub Server Name Server Groups.
   - Select Use this set of name servers to specify the default servers for the zone. Click the Add icon and specify the following:
     - Name: Enter a domain name of the server to which you want the NIOS appliance to forward queries.
     - Address: Enter the IP address of the server to which you want the NIOS appliance to forward queries.
     - Select Use Forwarders Only if you want the NIOS appliance to query forwarders only (not root servers) to resolve domain names in the zone.
5. Click Next to assign a forwarding member name server group or define Grid members to serve the forward-mapping zone. Select one of the following:

   Note: If you do not define any Grid members to serve the forward-mapping zone, then the named.conf file will not contain the configuration of the newly created forward zone. Hence, the Infoblox DNS server will not be authoritative to the forward zone and by default, the Infoblox DNS server will query the root servers to resolve queries for the forward zone.

   a. Select Use this name server group to assign a forwarding member NS group for the zone. You can select the forwarding member NS group from the drop-down list. For information about forwarding member NS groups, see Using Forwarding Member Name Server Groups.
   b. Select Use this set of name servers to define the Grid members and use the default forwarders or you can override default forwarders and configure custom forwarders. Click the Add icon to select the NIOS appliance on which the forward zone is configured. For an independent deployment, select the local appliance (it is the only choice). If there are multiple Grid members, the Member Selector dialog box is displayed. Select the required member by clicking the member name.

   The following is displayed for each Grid member:
   - Name: Displays the name of the Grid member.
   - IPv4 Address: Displays the IPv4 address of the Grid member.
   - IPv6 Address: Displays the IPv6 address of the Grid member.
   - Override Default Forwarders: Displays Yes when you override default forwarders. Otherwise, this field displays No.
   - Custom Forwarders: Displays the IP address of the custom forwarders. Otherwise, this field is blank.

   Note: Skip the following two steps if you want to use the default forwarders.

6. Select a member and click the Edit icon.
7. In the Edit Per-Member Forwarders editor, select the Override Default Forwarders check box to override the default forwarders. The Default Zone Forwarders table becomes available only after you select the Override Default Forwarders check box. Click the Add icon to specify the servers to which the NIOS appliance forwards queries for the zone:
   - Name: Enter a domain name for the server to which you want the NIOS appliance to forward queries for the specified domain name.
- **Address**: Enter the IP address of the server to which you want the NIOS appliance to forward queries.
- **Select Use Forwarders Only** if you want the NIOS appliance to query forwarders only (not root servers) to resolve domain names in the zone.
- **Save the configuration.** After successfully saving the configuration, the **Override Default Forwarders** column displays **Yes** and the **Custom Forwarders** column displays the IP address of the forwarders.
- To configure forwarders for multiple members, repeat the steps for each Grid member.

8. **Save the configuration**, or click **Next** to continue to the next step where you define extensible attributes as described in **Using Extensible Attributes**, and then optionally proceed to the next step where you define admin permissions as defined in **About Administrative Permissions**.

or

Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Tasks**.

9. **Click Restart** if it appears at the top of the screen.

To configure a forward IPv4 reverse-mapping zone:

1. From the **Data Management** tab, select the **Zones** tab, expand the Toolbar and click **Add -> Zone -> Add Forward Zone**.
2. In the **Add Forward Zone** wizard, click **Add a forward IPv4 reverse-mapping zone** and click **Next**.
3. Enter the following information, and then click **Next**:
   a. **IPv4 Network**: Enter the IPv4 address for the address space for which you want to define the reverse-mapping zone and select a netmask from the **Netmask** drop-down list. Alternatively, you can specify the address in CIDR format, such as 192/8.
   
   To use an RFC 2317 prefix, select a netmask value that is between 25 to 31, inclusive. Grid Manager displays the **RFC 2317 Prefix** field. Enter a prefix in the text field. Prefixes can be alphanumeric characters. For information, see **Specifying an RFC 2317 Prefix**.
   
   or
   
   **Name**: Enter the domain name of the reverse-mapping zone.
   
   To define the Grid members and use the default forwarders or you can override default forwarders and configure custom forwarders. Click the Add icon to select the NIOS appliance on which the forward zone is configured. For an independent deployment, select the local appliance (it is the only choice). If there are multiple Grid members, the Member Selector dialog box is displayed. Select the required member by clicking the member name.
   
   The following is displayed for each Grid member:
   - **Name**: Displays the name of the Grid member.
   - **IPv4 Address**: Displays the IPv4 address of the Grid member.
   - **IPv6 Address**: Displays the IPv6 address of the Grid member.
   - **Override Default Forwarders**: Displays **Yes** when you override default forwarders. Otherwise, this field displays **No**.
   - **Custom Forwarders**: Displays the IP address of the custom forwarders. Otherwise, this field is blank.

   **Note**: Skip the following two steps if you want to use the default forwarders.

4. **Click Next** to assign a forward/stub server name server group or define the default zone forwarders to which the NIOS appliance forwards queries for the zone. Select one of the following:
   - **Select Use this name server group** to assign or forward server NS group for the zone. You can select the forward/stub server NS group from the drop-down list. For information about forward/stub NS groups, see **Using Forward/Stub Server Name Server Groups**.
   - **Select Use this set of name servers** to specify the default servers for the zone. Click the Add icon and specify the following:
     - **Name**: Enter a domain name for the server to which you want the NIOS appliance to forward queries.
     - **Address**: Enter the IPv4 address of the server to which you want the NIOS appliance to forward queries.
     - **Override Default Forwarders**: Displays **Yes** when you override default forwarders. Otherwise, this field displays **No**.
     - **Custom Forwarders**: Displays the IP address of the custom forwarders. Otherwise, this field is blank.

5. **Click Next** to assign a forwarding member name server group or define Grid members to serve the forward-mapping zone. Select one of the following:
   - **Select Use this name server group** to assign a forwarding member NS group for the zone. You can select the forwarding member NS group from the drop-down list. For information about forwarding member NS groups, see **Using Forwarding Member Name Server Groups**.
   - **Select Use this set of name servers** to define the Grid members and use the default forwarders or you can override default forwarders and configure custom forwarders. Click the Add icon to select the NIOS appliance on which the forward zone is configured. For an independent deployment, select the local appliance (it is the only choice). If there are multiple Grid members, the Member Selector dialog box is displayed. Select the required member by clicking the member name.

The following is displayed for each Grid member:
   - **Name**: Displays the name of the Grid member.
   - **IPv4 Address**: Displays the IPv4 address of the Grid member.
   - **IPv6 Address**: Displays the IPv6 address of the Grid member.
   - **Override Default Forwarders**: Displays **Yes** when you override default forwarders. Otherwise, this field displays **No**.
   - **Custom Forwarders**: Displays the IP address of the custom forwarders. Otherwise, this field is blank.

6. **Select a member and click the Edit icon**.
7. **In the Edit Per-Member Forwarders editor**, select the **Override Default Forwarders** check box to override the default forwarders. The Default Zone Forwarders table becomes available only after you select the **Override Default Forwarders** check box. Click the Add icon to specify the servers to which the NIOS appliance forwards queries for the zone:
   - **Name**: Enter a domain name for the server to which you want the NIOS appliance to forward queries for the specified domain name.
   - **Address**: Enter the IPv4 address of the server to which you want the NIOS appliance to forward queries.
   - **Select Use Forwarders Only** if you want the NIOS appliance to query forwarders only (not root servers) to resolve domain names in the zone.
   - **Save the configuration**. After successfully saving the configuration, the **Override Default Forwarders** column displays **Yes** and the **Custom Forwarders** column displays the IP address of the forwarders.
To configure forwarders for multiple members, repeat the steps for each Grid member.

8. Save the configuration, or click Next to continue to the next step where you define extensible attributes as described in Using Extensible Attributes.

9. Click Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

To configure a forward IPv6 reverse-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Forward Zone.
2. In the Add Forward Zone wizard, click Add a forward IPv6 reverse-mapping zone and click Next.
3. Enter the following zone information:
   - IPv6 Network Address: Enter the 128-bit IPv6 address for the address space for which you want to define the reverse-mapping zone. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab::0:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered. Choose the network prefix that defines the IPv6 network address space.
   - Name: Enter the domain name of the reverse-mapping zone.
   - DNS View: This field displays only when there is more than one DNS view in the network view. Select a DNS view from the drop-down list.
   - Comment: Enter a descriptive comment about the zone.
   - Disable: Click this check box to temporarily disable this zone.
   - Lock: Click this check box to lock the zone so that you can make changes to it, and also prevent others making conflicting changes.

4. Click Next to assign a forward/stub server name server group or define the default zone forwarders to which the NIOS appliance forwards queries for the zone. Select one of the following:
   - Select Use this name server group to assign a forward/stub server NS group for the zone. You can select the forward/stub server NS group from the drop-down list. For information about forward/stub NS groups, see Using Forward/Stub Server Name Server Groups.
   - Select Use this set of name servers to specify the default servers for the zone. Click the Add icon and specify the following:
     - Name: Enter a domain name for the server to which you want the NIOS appliance to forward queries.
     - Address: Enter the IP address of the server to which you want the NIOS appliance to forward queries.
     - Select Use Forwarders Only if you want the NIOS appliance to query forwarders only (not root servers) to resolve domain names in the zone.

5. Click Next to assign a forwarding member name server group or define Grid members to serve the forward-mapping zone. Select one of the following:
   - Select Use this name server group to assign a forwarding member NS group for the zone. You can select the forwarding member NS group from the drop-down list. For information about forwarding member NS groups, see Using Forwarding Member Name Server Groups.
   - Select Use this set of name servers to define the Grid members and use the default forwarders or you can override default forwarders and configure custom forwarders. Click the Add icon to select the NIOS appliance on which the forward zone is configured. For an independent deployment, select the local appliance (it is the only choice). If there are multiple Grid members, the Member Selector dialog box is displayed. Select the required member by clicking the member name.

The following is displayed for each Grid member:
   - Name: Displays the name of the Grid member.
   - IPv4 Address: Displays the IPv4 address of the Grid member.
   - IPv6 Address: Displays the IPv6 address of the Grid member.
   - Override Default Forwarders: Displays Yes when you override default forwarders. Otherwise, this field displays No.
   - Custom Forwarders: Displays the IP address of the custom forwarders. Otherwise, this field is blank.

Configuring Stub Zones

A stub zone contains records that identify the authoritative name servers in the zone. It does not contain resource records for resolving IP addresses to hosts in the zone. Instead, it contains the following records:

- SOA (Start of Authority) record of the zone
- NS (name server) records at the apex of the stub zone
- A (Address) records that map the name servers to their IP addresses

Stub zones, like secondary zones, obtain their records from other name servers. Their records are read only; therefore, administrators do not
Stub zone records are also periodically refreshed, just like secondary zone records. However, secondary name servers contain a complete copy of the zone data on the primary server. Therefore, zone transfers from a primary server to a secondary server, or between secondary servers, can increase CPU usage and consume excessive bandwidth. A name server hosting a stub zone maintains a much smaller set of records; therefore, updates are less CPU intensive and consume less bandwidth.

When a name server hosting a stub zone receives a query for a domain name that it determines is in the stub zone, the name server uses the records in the stub zone to locate the correct name server to query, eliminating the need to query the root server. Figure 19.8 and Figure 19.9 illustrate how the NIOS appliance resolves a query for a domain name for which it is not authoritative. Figure 19.8 illustrates how the appliance resolves a query when it does not have a stub zone. Figure 19.9 illustrates how the appliance resolves the query with a stub zone.

In Figure 19.8, a client sends a query for ftp.sales.corp200.com to the NIOS appliance. When the appliance receives the request from the client, it checks if it has the data to resolve the query. If the appliance does not have the data, it tries to locate the authoritative name server for the requested domain name. It sends nonrecursive queries to a root name server and to the closest known name servers until it learns the correct authoritative name server to query.

In Figure 19.9, when the NIOS appliance receives the request for the domain name in corp200.com, it determines it does not have the resource records to resolve the query. It does, however, have a list of the authoritative name servers in the stub zone, corp200.com. The appliance then sends a query directly to the name server in corp200.com.

Figure 19.8 Processing a Query without a Stub Zone

Figure 19.9 Processing a Query with a Stub Zone
Stub zones facilitate name resolution and alleviate name server traffic in your network. For example, the client in the previous examples is in corpxyz.com. The corpxyz.com and corp200.com zones are partners, and send all their communications through a VPN tunnel, as shown in Figure 19.10. The firewall protecting corpxyz.com is configured to send all messages for the 10.2.2.0/24 network through the VPN tunnel. Infoblox_A hosts the stub zone for corp200.com. Therefore, when the host in corpxyz.com sends a query for ftp.sales.corp200.com, Infoblox_A obtains the IP address of Infoblox_B (10.2.2.7) from its stub zone records and sends the query to the firewall protecting corpxyz.com. Because the destination of the query is in the 10.2.2.0/24 network, the firewall (configured to encrypt all traffic to the network) sends the request through a VPN tunnel to Infoblox_B. Infoblox_B resolves the query and sends back the response through the VPN tunnel. All name server traffic went through the VPN tunnel to the internal servers, bypassing the root servers and external name servers.

In parent-child zone configurations, using stub zones also eases the administration of name servers in both zones. For example, as shown in Figure 19.10, sales.corp200.com is a child zone of corp200.com. On the corp200.com name servers, you can create either a delegated zone or a stub zone for sales.corp200.com. When you create a delegated zone, you must first specify the name servers in the delegated zone and manually maintain information about these name servers. For example, if the administrator in sales.corp200.com changes the IP address of a name server or adds a new name server, the sales.corp200.com administrator must inform the corp200.com administrator to make the corresponding changes in the delegated zone records. If, instead, you create a stub zone for sales.corp200.com, you set up the stub zone records once, and updates are then done automatically. The name servers in corp200.com that are hosting a stub zone for sales.corp200.com automatically obtain updates of the authoritative name servers in the child zone.

In addition, a name server that hosts a stub zone can cache the responses it receives. Therefore, when it receives a request for the same resource record, it can respond without querying another name server.

Creating Stub Zones
When you create a stub zone on the NIOS appliance, you specify the following:
• The Grid member that is hosting the stub zone

You can specify multiple appliances if you want the stub zones on multiple name servers. If you do, the appliances store identical records about the stub zone. You can also specify a stub member NS group for the zone. For information on specifying a stub member NS group, see Using Stub Member Name Server Groups.

• The IP address of the primary server(s) that the NIOS appliance can query in the stub zone

The primary server can be a Grid member or an external primary server. If you specify multiple primary servers, the appliance queries the primary servers, starting with the first server on the list. You can also specify a forward/stub server NS group for the zone. For information on specifying a forward/stub server NS group, see Using Forward/Stub Server Name Server Groups.

The primary server and the name server hosting the stub zone can belong to the same Grid, as long as the authoritative zone and the stub zone are in different DNS views. You cannot configure one zone as both authoritative and stub in the same view.

After you create a stub zone, the NIOS appliance does the following:

1. It sends a query to the primary server for the SOA (Start of Authority) record of the stub zone. The primary server returns the SOA record.
2. Then, it sends a query for the NS (name server) records in the zone.

The primary server returns the NS records and the A (address) records of the name servers. (These A records are also called glue records.)

If the primary server is a NIOS appliance, you might have to manually create the A record and add it to the stub zone. A NIOS appliance that is the primary server for a zone always creates an NS record, but does not always create an A record.

• The appliance automatically creates an A record when its host name belongs to the name space of the zone. For example, if the zone is corpxyz.com and the primary server host name is server1.corpxyz.com, the appliance automatically creates the NS and A records and sends these records when it is queried by the stub zone name server.

• The appliance does not automatically create an A record when its host name is in a name space that is different from the zone. For example, if the zone is corp200.com and the primary server host name is server1.corp200.com, then the appliance creates the NS record only and sends it when it is queried by the stub zone name server. In this case, you must manually create the A record.

Maintaining Stub Zones

The NIOS appliance maintains the stub zone records and updates them based on the values in the SOA record as follows:

• The refresh interval indicates when the appliance sends a discrete query to the primary name server for the stub zone. The appliance learns about any changes in the stub zone and updates the NS and A records in the stub zone accordingly.
• If the update fails, the retry interval indicates when the appliance resends a discrete query.
• If the query continues to fail, the expiry value indicates when the appliance stops using the zone data.

Adding Stub Zones

To add a stub zone, you must identify the Infoblox appliance that hosts the stub zone, and provide the IP address of the primary server. You can also add stub zones for Microsoft servers that are managed by Grid members. For information, see Managing Microsoft Windows Servers.

You can configure a stub zone for forward mapping or reverse mapping zones.

To add a forward-mapping stub zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Stub Zone.
2. In the Add Stub Zone wizard, click Add a stub forward-mapping zone and click Next.
3. Specify the following, and then click Next:
   • Name: Enter the name for the stub zone.
   • Comment: Enter a useful comment, such as the admin to contact for the stub zone.
   • Disable: Click this check box to temporarily disable this zone.
   • Lock: Click this check box to lock the zone so that you can make changes to it, and also prevent others from making conflicting changes.
4. Click Next to define primary servers in the stub zone. You can specify a forward/stub server NS group or define the servers individually. Select one of the following:

   • Select Use this name server group to assign a forward/stub server NS group for the stub zone. You can select the forward/stub server NS group from the drop-down list. For information about forward/stub server NS groups, see Using Forward/Stub Server Name Server Groups.
   • Select Use this set of name servers to define primary servers for the stub zone. Click the Add icon and enter the Name and IP Address of the primary server in the stub zone.

If the primary server is a Grid member, you must enter the host name and IP address of the Grid member. The NIOS appliance does not validate these entries. Therefore, if you change the IP address of a Grid member listed here, you must update the Grid member information in this list as well.

You can specify multiple primary servers for redundancy. If the primary server is a NIOS appliance, the appliance must have the Minimal Response feature disabled so it can propagate the data to the stub server. For information about the Minimal Response feature, see Specifying Minimal Responses.

Optionally, click the Don't use forwarders to resolve queries in subzones check box to indicate that the name servers hosting the stub zone must not use forwarders to resolve queries for domain names in the stub zone or in its subzones.

5. Click Next to specify a stub member NS group or define the name servers individually to serve the forward-mapping stub zone. Select one of the following:
You can define two types of reverse-mapping stub zones, one for IPv4 addresses and one for IPv6 addresses. To configure an IPv4 reverse-mapping stub zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Stub Zone.
2. In the Add Stub Zone wizard, click Add a stub IPv4 reverse-mapping zone and click Next.
3. Specify the following:
   - IPv4 Network: Enter the IPv4 address for the address space for which you want to define the reverse-mapping zone and select a netmask from the Netmask drop-down list. Alternatively, you can specify the address in CIDR format, such as 192/8.
   - To use an RFC 2317 prefix, select a netmask value that is between 25 to 31, inclusive. Grid Manager displays the RFC 2317 Prefix field. Enter a prefix in the text field. Prefixes can be alphanumeric characters. For information, see Specifying an RFC 2317 Prefix.
   - or
   - Name: Enter the domain name of the reverse-mapping zone.
   - DNS View: This field displays only when there is more than one DNS view in the network view. Select a DNS view from the drop-down list.
   - Comment: Optionally, enter additional information about the zone.
   - Disable: Click this check box to temporarily disable this zone.
   - Lock: Click this check box to lock the zone so that you can make changes to it, and also prevent others from making conflicting changes.
4. Click Next to define primary servers in the stub zone. You can specify a forward/stub server NS group or define the servers individually. Select one of the following:
   - Select Use this name server group to assign a forward/stub server NS group for the stub zone. You can select the forward/stub server NS group from the drop-down list. For information about forward/stub server NS group, see Using Forward/Stub Server Name Server Groups.
   - Select Use this set of name servers to define primary servers for the stub zone. Click the Add icon and enter the Name and IP Address of the primary server in the stub zone.
     - If the primary server is a Grid member, you must enter the host name and IP address of the Grid member. The NIOS appliance does not validate these entries. Therefore, if you change the IP address of a Grid member listed here, you must update the Grid member information in this list as well.
     - You can specify multiple primary servers for redundancy. If the primary server is a NIOS appliance, the appliance must have the Minimal Response feature disabled so it can propagate the data to the stub server. For information about the Minimal Response feature, see Specifying Minimal Responses.
     - Optionally, click the Don't use forwarders to resolve queries in subzones check box to indicate that the name servers hosting the stub zone should not forward queries that end with the domain name of the stub zone to any configured forwarders.
5. Click Next to specify a stub member NS group or define the name servers individually to serve the reverse-mapping stub zone. Select one of the following:
   - Select Use this name server group to assign a stub member NS group for the zone. You can select the forward/stub server NS group from the drop-down list. For information about stub member NS group, see Using Stub Member Name Server Groups.
   - Select Use this set of name servers to define the servers individually. Click the Add icon and select one of the following:
     - Add Infoblox Member: Select this and select the Grid member that hosts the stub zone.
     - Name: Displays the name of the name server.
     - IPv4 Address: Displays the IPv4 address of the name server.
     - IPv6 Address: Displays the IPv6 address of the name server.
6. Click Next to continue to the next step where you define extensible attributes as described in Using Extensible Attributes.
7. Save the configuration and click Restart if it appears at the top of the screen or Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

To configure an IPv6 reverse-mapping stub zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Stub Zone.
2. In the Add Stub Zone wizard, click Add a stub IPv6 reverse-mapping zone and click Next.
3. Specify the following:
- **IPv6 Network Prefix and Prefix Length**: Enter the 128-bit IPv6 address for the address space for which you want to define the reverse-mapping zone. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab:0:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered. You can enter a slash and prefix length in the IPv6 Network Prefix field or you can choose a value from the Prefix Length drop-down list.

- **Name**: Enter the domain name of the reverse-mapping zone.
- **DNS View**: This field displays only when there is more than one DNS view in the current network view. Select a DNS view from the drop-down list.
- **Comment**: Enter a descriptive comment about the zone.
- **Disable**: Click this check box to temporarily disable this zone.
- **Lock**: Click this check box to lock the zone so that you can make changes to it and prevent others from making conflicting changes.

4. Click **Next** to define primary servers in the stub zone. You can specify a forward/stub server NS group or define the servers individually. Select one of the following:

- **Select Use this name server group** to assign a forward/stub server NS group for the stub zone. You can select the forward/stub server NS group from the drop-down list. For information about forward/stub server NS group, see **Using Forward/Stub Server Name Server Groups**.
- **Select Use this set of name servers** to define primary servers for the stub zone. Click the Add icon and enter the **Name** and **IPv4 Address** of the primary server in the stub zone. If the primary server is a Grid member, you must enter the host name and IP address of the Grid member. The NIOS appliance does not validate these entries. Therefore, if you change the IP address of a Grid member listed here, you must update the Grid member information in this list as well. You can specify multiple primary servers for redundancy. If the primary server is a NIOS appliance, the appliance must have the **Minimal Response feature** disabled so it can propagate the data to the stub server. For information about the Minimal Response feature, see **Specifying Minimal Responses**.

5. Click **Next** to specify a stub member NS group or define the name servers individually to serve the reverse-mapping stub zone. Select one of the following:

- **Select Use this name server group** to assign a stub member NS group for the zone. You can select the stub member NS group from the drop-down list. For information about stub member NS group, see **Using Stub Member Name Server Groups**.
- **Select Use this set of name servers** to define the servers individually. Click the Add icon and select one of the following:
  - **Add Microsoft Server**: Select this and select the Microsoft server that hosts the stub zone. The following is displayed for each name server:
    - **Name**: Displays the name of the name server.
    - **IPv4 Address**: Displays the IPv4 address of the name server.
    - **IPv6 Address**: Displays the IPv6 address of the name server.

6. Click **Next** to continue to the next step where you define extensible attributes as described in **Using Extensible Attributes**.

7. Save the configuration and click **Restart** if it appears at the top of the screen or click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Tasks**.

**Viewing and Modifying SOA Records**

The timer values in the SOA record determine when the zone data is updated. The MNAME field and the RNAME field of the SOA record display the FQDN of the primary server and the administrative email address respectively. You can view these default values and override them when necessary. For a zone that has multiple primary servers, Grid Manager displays all configured primaries for the zone. You can click **Override** to override the Grid-level settings. If the primary server is a Microsoft server however, the **Override** option does not appear. You can only change certain values in the SOA record.

To view and modify zone SOA record values:

1. From the **Data Management** tab, select the DNS tab -> Zones tab -> zone check box, and then click the **Edit** icon.
2. In the **Authoritative Zone or Stub Zone** editor, click the **Settings** tab to view the following values. You can also click **Override** to modify some of the values.

- **Serial number**: The current serial number for the primary server. This number is automatically increased when changes are made to the zone or its record. The serial number plays a key role in determining when and whether zone data is updated. You can change the serial number only if the primary server of the zone is a Grid member. When the zone has multiple primary servers, each primary can have its own serial number. In this case, the serial number displayed here is always that of the Grid Master, which will also appear in the primary name server list if it is one of the primaries for the zone.

  **Note**: If you change the serial number of the Grid Master, serial numbers for all primaries will be changed to the same number. A warning is displayed when you try to decrement the serial number.
• **Refresh:** This interval tells secondary servers how often to send a message to the primary server for a zone to check that their data is current, and retrieve fresh data if it is not. The default is three hours.
• **Retry:** This interval tells the secondary server how long to wait before attempting to recontact the primary server after a connection failure between the two occurs. The default is one hour.
• **Expire:** If the secondary fails to contact the primary for the specified interval, the secondary stops giving out answers about the zone because the zone data is too old to be useful. The default is 30 days.
• **Default TTL:** Specifies how long name servers can cache the data. The default is eight hours.
• **Negative-caching TTL (Time to Live):** Specifies how long name servers can cache negative responses. The default is 15 minutes.
• **Primary name server (for SOA MNAME field):** If the primary name server of a zone is a Grid member, the MNAME is inherited from its corresponding member, and you can change the name of the primary name server that is published in the MNAME field of the SOA record. This field accepts names in native character sets. If the zone has multiple primary name servers, a list of all primaries is displayed in this section. Each primary has its own serial number and the number can be different among them. Note that the serial numbers for these primaries are read-only and you cannot modify them. If you change the serial number of the Grid Master, serial numbers for all primaries will be changed to the same number.
• **Email Address (for SOA RNAME field):** If the primary name server of a zone is a Grid member, you can enter an administrator email address to the SOA record to help people determine who to contact about this zone. The appliance supports IDN for the host name of the Email address. For example, you can create admin@. but not @.com.
• **Don’t use forwarders to resolve queries in subzones:** Select this option to disable the use of forwarders to resolve queries for data in subzones.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

To schedule this task, click the Schedule icon at the top of the wizard. In the Schedule Change panel, click **Later**, and then specify a date, time, and time zone. The Schedule icon is green when there is a pending scheduled task. You can reschedule the task if you have the applicable permissions.

**Configuration Example: Configuring a Stub Zone in a Grid**

This example illustrates how to configure a stub zone and assign it to a Grid member. You configure a Grid, corpxyz, with a single Grid Master and Grid member. The Grid member, member1.corpxyz.com, is the primary name server for the corpxyz.com zone in the internal view. The Grid Master, gm-corpxyz.com, hosts the stub zone for corpxyz.com in the external view. Thus, when the Grid Master receives a query for the corpxyz.com zone, it sends it directly to member1.corpxyz.com, the primary name server for the zone.

In this example, you configure the following:

1. Turn off minimal responses on member1.corpxyz.com, the primary name server for the corpxyz.com zone. See Disable Minimal Responses.
2. Create the internal and external views. See Create the Views.
3. Create the corpxyz.com authoritative zone and stub zone. See Create the Zones.

**Disable Minimal Responses**

After you create the Grid, turn off minimal responses for member1.corpxyz.com. Disabling minimal responses ensures that member1.corpxyz.com propagates the required data to the server hosting the stub zone.

1. From the Data Management tab, select the DNS tab, click Members -> member1.corpxyz.com check box -> Edit icon.
2. In the Member DNS Configuration editor, click the General -> Basic tab.
3. Clear the Return minimal responses check box.
4. Save the configuration and click Restart if it appears at the top of the screen.

**Create the Views**

Create the internal and external views. To create each view:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add DNS View.
2. In the Add DNS View wizard, enter the name of the view. In this example, enter either External or Internal.
3. Click Save & New and create the other DNS view.

**Create the Zones**

Create the corpxyz.com zone in the internal view and assign member1.corpxyz.com as the Grid primary server:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Auth Zone.
2. In the Forward Authoritative Zone wizard, do the following:
   - Select Add an authoritative forward-mapping zone and click Next.
   - Enter the zone name, corpxyz.com and select the Internal DNS view. Click Next.
   - Select Use this set of name servers and select member1.corpxyz.com as the Grid primary server.
3. Save the configuration and click Restart if it appears at the top of the screen.

After you create the zone, you can view the NS and A records which were automatically created.

Create the stub zone, corpxyz.com, in the external view, assign gm-corpxyz.com as the stub member and member1.corpxyz.com as the stub primary server.

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Zone -> Add Stub Zone.
2. In the Stub Zone wizard, do the following:
   - Select Add a stub forward-mapping zone and click Next.
   - Enter the name of the stub zone, corpxyz.com and select the External DNS view. Click Next.
   - In the Master Name Servers panel, click the Add icon and enter the following for the primary name server, and then click Next:
     - Name: member1.corpxyz.com
     - Address: 10.35.0.222
   - In the Name Servers panel, click the Add icon and select gm-corpxyz.com.
   - Save the configuration and click Restart if it appears at the top of the screen.

After you create the stub zone, the server hosting the stub zone, gm-corpxyz.com, sends queries to the primary server, member1.corpxyz.com, for the SOA and NS records. member1.corpxyz.com then returns its NS records and A (address) records.

**Viewing Zones**

To list zones, navigate to the Data Management tab -> DNS tab -> Zones panel. If there is more than one DNS view in the Grid, this panel lists the DNS views. Select a DNS view to list its zones. (For information, see Listing DNS Views.)

- Click Toggle flat view to display a flat list of all the zones in the view.
- Click Toggle hierarchical view to display only the apex zones.

In the hierarchical view, you can see one entry for the host that represents the entire host object. In a host record, there can be multiple DNS resource records (A, PTR, CNAME) and some DHCP data (fixed addresses) as well. In the flat view, each of the DNS resource records in the host are listed separately.

For example, the host called server1.infoblox.com contains 2 A records and an ALIAS (which is a host naming convention for CNAME records). If you view the infoblox.com zone using the hierarchical view option, you will see one entry host for server1.infoblox.com. In the flat view, you will see three records (one for each IP address/A record, and one host Alias for the CNAME). In the flat view, you cannot delete one piece of the host record. You can edit the host record and you can remove information. Deleting host records deletes the entire host record only.

This panel displays the following information for each zone, by default:

- **Name**: The domain name of the zone.
- **MS Sync Server**: When a zone is served by multiple Microsoft servers, this column shows which Microsoft server is actually performing the synchronization of that zone with the Grid.
- **MS Zone Sync**: Displays Yes if you have enabled zone synchronization, and displays No when the zone synchronization is disabled.
- **Grid Primary Server**: The primary name server configured for an authoritative zone in the DNS view.
- **Type**: The zone type. Possible values are Authoritative, Forward, Stub and Delegation.
- **Multi-masterZone**: Indicates whether this zone has multiple primary name servers.
- **Comment**: Comments that were entered for the zone.
- **Site**: Values that were entered for this pre-defined attribute.

You can also display the following columns:

- **Locked**: Displays Yes when a zone is locked by an admin, and displays No when the zone is unlocked.
- **Function**: Indicates whether the zone is a forward-mapping, or an IPv4 or IPv6 reverse-mapping zone.
- **ZSK rollover date**: Displays the date when the ZSK is due for next rollover. The appliance performs a rollover automatically at this time.
- **KSK rollover date**: Displays the date when the KSK is due for next rollover. The appliance performs a rollover automatically at this time if you have enabled automatic KSK rollover. For more information, see Configuring Automatic KSK Rollovers and Notifications. You must perform the rollover manually, if you have disabled this option.
- **Disabled**: This field displays Yes if the zone is disabled. Otherwise, this field displays No.
- **Signed**: This field displays Yes if the zone is a DNSSEC-signed zone. Otherwise, this field displays No. You can do the following:
- List the resource records and subzones of a DNS zone.
- Click a DNS zone name.
- Use filters and the Goto function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Goto field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
- Edit the properties of a DNS zone.
- Click the check box beside a DNS zone, and then click the Edit icon.
- Delete a DNS zone.
- Export the list of DNS zones to a .csv file.
- Print the list of DNS zones.
- Click the Print icon.

**About Name Server Groups**

NS (name server) group is a collection of one or more DNS servers. Grouping a commonly used set of DNS servers together simplifies zone creation by enabling you to specify a single NS group instead of specifying multiple name servers individually. You can configure the following types of NS groups:

- **Authoritative NS Group**—For information, see Using Authoritative Name Server Groups.
- **Delegation NS Group**—For information, see Using Delegation Name Server Groups.

Copyright ©2019, Infoblox, Inc. All right reserved.
• Forwarding Member NS Group—For information, see Using Forwarding Member Name Server Groups.
• Stub Member NS Group—For information, see Using Stub Member Name Server Groups.
• Forward/Stub Server NS Group—For information, see Using Forward/Stub Server Name Server Groups.

Using Authoritative Name Server Groups

An authoritative NS (name server) group is a collection of one or more primary DNS servers and secondary DNS servers. After you create an authoritative NS group, you can then assign it to serve authoritative forward-mapping and reverse-mapping zones. When you assign an authoritative NS group to an authoritative zone, Grid Manager automatically generates an NS record, a glue A or AAAA record, and a PTR record for each name server available in the NS group. But if the zone is disabled, Grid Manager does not generate these records.

Grid Manager generates authoritative A, AAAA, and PTR records when:

• A Grid member is added to a Grid, whose host name belongs to the name space of the authoritative zone and vice versa.
• An external name server is assigned to a zone, whose host name belongs to the name space of the authoritative zone.

Note: Grid Manager does not generate an NS record when the DNS service for the member is disabled.

The performance of the following functions significantly improve when you assign an NS group to a zone instead of specifying multiple name servers individually:

• Starting and Stopping the DNS service.
• Reparenting the zones after removing or restoring a zone.
• Modifying the zone data.

Note: Only superusers can create and manage name server groups.

Adding Authoritative Name Server Groups

To add an authoritative name server group:

1. From the Data Management -> DNS tab, do one of the following:
   • Click the Name Server Groups tab -> Add icon -> Group -> Authoritative.
   • From the Toolbar, click the Add icon -> Group -> Authoritative.

2. In the Add Name Server Group wizard, do the following:
   • Name: Type a name that provides a meaningful reference for this set of servers.
   • Name Servers: Click the Add icon and select one of the following options for every server that you are adding to the NS group:
     • Grid Primary: Choose this option to select a primary name server or multiple primary servers for the zone. See Specifying Grid Primary Servers.
     • Grid Secondary: Choose this option to select a Grid member as a secondary server for the zone. See Adding Grid Secondaries.
     • External Primary: Choose this option if the appliance is in a Grid and you want to specify a primary server outside the Grid ("external" to the Grid). See Specifying External Primary Servers.
     • External Secondary: Choose this option if the appliance is in a Grid and you want to specify a secondary server outside the Grid ("external" to the Grid), or if the appliance is deployed independently from a Grid. See Specifying External Secondaries.
   • Default NS Group: Select this to specify this authoritative name server group as the default.
   • Comment: Optionally, enter additional information about the authoritative NS group.

3. Save the configuration and click Restart if it appears at the top of the screen, or click Next to define extensible attributes. For information, see Using Extensible Attributes.

A newly created authoritative name server group appears in the Name Server Groups tab. For information about viewing the name server groups, see Viewing Name Server Groups. You can then associate it with forward-mapping and reverse-mapping authoritative zones.

Applying Authoritative Name Server Groups

In Grid Manager, you can assign an authoritative name server group to an authoritative zone when you first create it using the Add Authoritative Zone wizard and when you edit an existing authoritative zone using the Authoritative Zone editor. For information on creating an authoritative zone using the wizard, see Configuring Authoritative Zones. The panels used to assign a name server group to a zone are the same in the wizard or and editor. The only difference is the way you access it. The following procedure describes how to specify an authoritative NS group when editing a forward-mapping zone:

1. From the Data Management tab -> DNS tab -> Zones tab -> zone check box, and then click the Edit icon.
2. In the Authoritative Zone editor, click Name Servers.
3. Select Use this name server group, and then select the authoritative NS group from the drop-down list.
Note: If you apply a name server group to at least one zone or specify it as the default group, you cannot rename or remove it. To rename or remove a group, you must first disassociate it from all zones and unassign it as the default group.

Using Delegation Name Server Groups

Delegation NS (Name Server) group is a collection of external name servers for delegated zones. Adding a set of external name servers to a single delegation NS group can significantly reduce configuration efforts. While configuring delegated zones, you can specify a single delegation NS group instead of configuring multiple name servers individually. After you create a delegation NS group, you can then assign it to serve only delegated zones. When you assign a delegation NS group to a delegated zone, Grid Manager automatically generates an NS record, a glue A or AAAA record, and a PTR record for each name server available in the delegation NS group. But if the zone is disabled, Grid Manager does not generate these records.

Note the following while adding a delegation NS group:

- You cannot add a delegation NS group if a NS group with the same name already exists and vice versa.
- If a Grid has any Microsoft servers configured, delegation NS groups are not allowed and vice versa.
- You cannot delete a delegation NS group if it is assigned to a zone.
- The DNS server resolves the FQDN of the delegated name server and does not use the IP address that you specify when assigning the delegated name servers.

Adding Delegation Name Server Groups

To add a delegation name server group:

1. From the Data Management -> DNS tab, do one of the following:
   - Click the Name Server Groups tab -> Add icon -> Delegation.
   - From the Toolbar, click the Add icon -> Group -> Delegation.
2. In the Add Delegation Name Server Group wizard, complete the following:
   - Name: Enter the name of the delegation NS group.
   - Comment: Optionally, enter additional information about the delegation NS group.
3. Click Next to define the external name servers for the delegation NS group.
4. In the Name Server panel, click the Add icon and specify the following for every server that you are adding to the delegation NS group:
   - Name: Enter the name of the delegated name server.
   - Address: Enter the IP address of the delegated name server.
5. Save the configuration and click Restart if it appears at the top of the screen, or click Next to define extensible attributes. For information, see Using Extensible Attributes.

A newly created delegation NS group appears in the Name Server Groups tab. For information about viewing the name server groups, see Viewing Name Server Groups. You can then associate it with delegated zones.

Applying Delegation Name Server Groups

You can assign a delegation NS group to a delegated zone when you first create it using the Add Delegation wizard and when you edit an existing delegated zone using the Delegation Zone editor. For information about creating a delegated zone using the wizard, see Configuring a Delegation.

Complete the following to assign a delegation NS group to a delegation zone:

1. From the Data Management tab -> DNS tab -> Zones tab -> delegation zone check box, and then click the Edit icon.
2. In the Delegation Zone editor, click Delegated Name Servers.
3. Select Use this name server group, and then select the delegation NS group from the drop-down list.

Using Forwarding Member Name Server Groups

A forwarding member NS (Name Server) group is a collection of one or more forwarding name servers. Grouping a set of forwarding name servers together reduces the configuration efforts. When you configure a forwarding zone, you can specify a single forwarding member NS group instead of specifying multiple forwarding name servers individually. After you create a forwarding member NS group, you can assign it to a forward forward-mapping zone and a forward reverse-mapping zone.

Note the following while adding a forwarding member NS group:

- Only superusers can add, modify, and delete a forwarding member NS group.
- You cannot add a forwarding member NS group if a NS group with the same name already exists and vice versa.
- You cannot delete a forwarding member NS group if it is assigned to a zone.

Adding Forwarding Member Name Server Groups

To add a forwarding member NS group:

1. From the Data Management -> DNS tab, do one of the following:
Applying Stub Member Name Server Groups

A stub member NS (Name Server) Group is a collection of one or more Grid members for stub zones. When you configure a stub zone, you can specify a single stub member NS group instead of specifying multiple Grid members individually, thus reducing the configuration efforts. After you create a stub member NS group, you can assign it to forward-mapping stub zones and reverse-mapping stub zones.

Note the following while adding a stub member NS group:

- Only superusers can add, modify, and delete a stub member NS group.
- You cannot add a stub member NS group if a NS group with the same name already exists and vice versa.
- You cannot delete a stub member NS group if it is assigned to a zone.

Adding Stub Member Name Server Groups

To add a stub member NS group:

1. From the Data Management tab -> DNS tab, do one of the following:
   - Click the Name Server Groups tab -> Add icon -> Stub Member.
   - From the Toolbar, click the Add icon -> Group -> Stub Member.
2. In the Stub Member Name Server Group wizard, complete the following:
   - Name: Enter the name of the stub member NS group.
   - Name Servers: In this section, you can add the Grid members to the stub member NS group. Click the Add icon and select a Grid member from the MemberSelector dialog box.
     The following is displayed in the table for each member:
     - Name: The name of the Grid member.
     - IPv4Address: The IPv4 address of the Grid member.
     - IPv6Address: The IPv6 address of the Grid member.
     - Override Default Forwarders: Displays Yes when you override default forwarders. Otherwise, this field displays No.
     - Custom Forwarders: Displays the IP address of the custom forwarders. Otherwise, this field is blank.
   - Comment: Optionally, enter additional information about the stub member NS group.
3. Save the configuration or click Next to define extensible attributes. For information, see Using Extensible Attributes.

A newly created stub member NS group appears in the Name Server Groups tab. For information about viewing the name server groups, see Viewing Name Server Groups. You can then associate it with forward-forward-mapping zones and forward reverse-mapping zones.

Applying Stub Member Name Server Groups

You can assign a stub member NS group to a stub zone when you first create it using the Add Stub Zone wizard and when you edit an existing stub zone using the Stub Zone editor. For information about creating a stub zone using the wizard, see Configuring Stub Zones.

Complete the following to assign a stub member NS group to a stub zone:

1. In the forward-mapping zones and stub reverse-mapping zones.

Copyright ©2019, Infoblox, Inc. All right reserved.
1. From the **Data Management** tab -> **DNS** tab -> **Zones** tab -> *stub zone* check box, and then click the Edit icon.
2. In the **Stub Zone** editor, click **Name Servers**.
3. Select **Use this name server group**, and then select the stub member NS group from the drop-down list.

### Using Forward/Stub Server Name Server Groups

A forward/stub server NS (Name Server) group is a collection of one or more external name servers. Grouping a set of external name servers together to a forward/stub server NS group reduces the configuration efforts. You can assign a single forward/stub server NS group as default forwarders for a forward zone or as primary servers for a stub zone instead of specifying multiple name servers individually. Note the following while adding a forward/stub server NS group:

- Only super-users can add, modify, and delete a forward/stub server NS group.
- You cannot add a forward/stub server NS group if a NS group with the same name already exists and vice versa.
- You cannot delete a forward/stub server NS group if it is assigned to a zone.

### Adding Forward/Stub Server Name Server Groups

To add a forward/stub server NS group:

1. From the **Data Management** -> **DNS** tab, do one of the following:
   - Click the **Name Server Groups** tab -> Add icon -> **Forward/Stub Server**.
   - From the Toolbar, click the Add icon -> **Group** -> **Forward/Stub Server**.
2. In the **Forward/Stub Server Name Server Group** wizard, complete the following:
   - **Name**: Enter a name that provides a meaningful reference for this set of external name servers for the forward and stub zones.
   - **Name Servers**: Click the Add icon and specify the following for every external name server that you are adding to the forward/stub server NS group:
     - **Name**: The name of the external name server.
     - **IP Address**: The IP address of the external name server.
     - **Comment**: Optionally, enter additional information about the forward/stub server NS group.
3. Save the configuration or click **Next** to define extensible attributes. For information, see Using Extensible Attributes.

A newly created forward/stub server NS group appears in the **Name Server Groups** tab. For information about viewing the name server groups, see Viewing Name Server Groups. You can then associate it with forward zones as default forwarders and as primary servers for stub zones.

### Applying Forward/Stub Server Name Server Groups

You can assign a forward/stub server NS group to a forward zone as default forwarders and as primary servers to a stub zone when you first create it and when you edit an existing forward zone and stub zone. For information about creating a forward zone using the wizard, see Configuring a Forward Zone. For information about creating a stub zone using the wizard, see Configuring Stub Zones.

Complete the following to assign a forward/stub server NS group to a forward zone:

1. From the **Data Management** tab -> **DNS** tab -> **Zones** tab -> **forward zone** check box, and then click the Edit icon.
2. In the **Forward Zone** editor, click **Forwarders**.
3. Select **Use this name server group**, and then select the forward/stub server NS group from the drop-down list. Complete the following to assign a forward/stub server NS group to a stub zone:
4. From the **Data Management** tab -> **DNS** tab -> **Zones** tab -> **stub zone** check box, and then click the Edit icon.
5. In the **Stub Zone** editor, click **Masters**.
6. Select **Use this name server group**, and then select the forward/stub server NS group from the drop-down list.

### Viewing Name Server Groups

You can view the configured authoritative, delegation, forwarding member, stub member, and forward/stub server name server groups by navigating to the **Data Management** tab -> **DNS** tab -> **Name Server Groups** tab.

The panel displays the following information about each name server group:

- **Name**: The name of the name server group.
- **Type**: The name server group type. Possible values are **Authoritative**, **Delegation**, **Forwarding Member**, **Stub Member**, and **Forward/Stub Server**.
- **Comment**: Comments that were entered for the name server group.
- **Site**: Values that were entered for this pre-defined attribute. You can do the following:
  - Use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.
  - Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
  - Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
- **Edit the properties of a name server group.**
  - Select the check box beside a name server group, and then click the Edit icon.
- **Delete a name server group.**
  - Select the check box beside a name server group, and then click the Delete icon. Note that you cannot delete a delegation name...
server group that is assigned to a zone.

- Export the list of Grid members to a .csv file.
  - Click the Export icon.
- Print the list of Grid members.
  - Click the Print icon.

Chapter 20 DNS Resource Records

This chapter provides general information about Infoblox host records and DNS resource records. The topics in this chapter include:

- About Bulk Hosts
  - Specifying Bulk Host Name Formats
  - Before Defining Bulk Host Name Formats
  - Adding Bulk Hosts
- Managing Resource Records
  - Managing A Records
  - Managing NS Records
  - Managing AAAA Records
  - Managing PTR Records
  - Managing MX Records
  - Managing SRV Records
  - Managing TXT Records
  - Managing sized Records
  - Managing TSIG Records
  - Managing CNAME Records
  - Managing DNAME Records
  - Managing NAPTR Records
  - Managing LBDN Records
  - Viewing Resource Records
  - Modifying, Disabling, and Deleting Host and Resource Records
- About Shared Record Groups
  - Shared Records Guidelines
  - Configuring Shared Record Groups
  - Managing Shared Resource Records
  - Managing Associated Zones
  - Configuration Example: Configuring Shared Records

About Bulk Hosts

If you need to add a large number of A and PTR records, you can have the NIOS appliance add them as a group and automatically assign host names based on a range of IP addresses and the host name format you specify. Such a group of records is called a bulk host, which the appliance manages and displays as a single bulk host record.

Specifying Bulk Host Name Formats

Bulk host name formats provide a flexible way to define bulk host names. You create multiple bulk host formats at the Grid level. Either select from the default bulk host formats or create your own. You can specify a different format for each bulk host. When you assign a bulk host name format to a bulk host in a zone, the system applies the zone's host name policy to it. It can also be blank. The suffix is derived from an IP address in the bulk host IP address range. The appliance also supports IDNs for bulk host names. You can use IDNs or their punycode representations while creating bulk hosts.

The following table summarizes how the appliance displays bulk host names that contain IDNs:

<table>
<thead>
<tr>
<th>Input</th>
<th>NIOS Displays...</th>
<th>NIOS DNS Domain (Punycode in the GUI)</th>
<th>Conversion Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello</td>
<td>hello</td>
<td>hello</td>
<td>No conversion</td>
</tr>
<tr>
<td>xn--80ad5k5aih3fr9e</td>
<td>xn--80ad5k5aih3fr9e</td>
<td>xn--80ad5k5aih3fr9e</td>
<td>IDN to punycode</td>
</tr>
<tr>
<td>\xyz format</td>
<td>\xyz format</td>
<td>\xyz format</td>
<td>No conversion</td>
</tr>
</tbody>
</table>

The suffix format is a string of ASCII characters that uses $ (unpadded) or # (zero-padded) followed by 1,2,3,4 to refer to the first, second, third, or fourth IP address octet; it uses $1,$2,$3,$4 or #1,#2,#3,#4. $2 refers to the second unpadded octet and #4 refers to the fourth zero-padded octet. For example:

The prefix of a bulk host = info IP address = 10.19.32.133 Domain name = infoblox.com.

If you specify the default four-octet format $4-$2-$3-$4, the bulk host name is info-10-19-32-133.infoblox.com.

If you specify a custom name format such as #1#2#3#4, the bulk host name is info*010*019*023*133.infoblox.com.
Before Defining Bulk Host Name Formats
Before you specify a bulk host name format, ensure that it complies with the following rules:

- The NIOS appliance uses <prefix>-xx-xx-xx-xx for bulk hosts. Ensure that the bulk host name does not conflict with CNAMEs, DNAMEs, or host name aliases.
- When you add a bulk host, if you enable the Automatically add reverse mapping option and there is a CNAME record in the corresponding reverse zone that conflicts with a PTR record generated by the bulk host, the bulk host insertion fails and an error message appears. For example, if there is a CNAME with the alias 15 in a reverse zone 1.168.192.in-addr.arpa and if you add a bulk host foo/192.168.1.10/192.168.1.20 with the Automatically add reverse mapping option selected, the insertion fails and an error message appears because both the bulk host and the CNAME generate a record 15.1.168.192.in-addr.arpa in the reverse zone.
- You cannot create or change a bulk host if a zone is locked by another user. If you select a different template for the Grid, it changes each record associated with the bulk host.
- You can define bulk host name formats only at the Grid level and override them at the bulk host level; not at the zone or bulk host object level.
- When you upgrade to NIOS 4.3/3 or earlier releases, the system migrates existing bulk hosts as follows:
  - If you did not customize the bulk host IP format, there is no action required. All migrated bulk hosts continue to use the Grid-level default four-octet format $2-$3-$4-$5. See Specifying Bulk Host Name Formats.
  - If you customized the bulk host IP format, the system creates a new template called Migrated Default. All migrated bulk hosts override the Grid default template and use the Migrated Default template.

Note: The NIOS appliance considers two bulk hosts that have the same prefix, start address, and end address as duplicate hosts; even if they use different bulk host formats.

Bulk Host Name Format Rules
Table 20.1 describes the rules that you should follow when you create bulk host name formats. It also provides examples of valid and invalid formats for each rule.

Table 20.1 Bulk Host Name Format Rules and Examples

<table>
<thead>
<tr>
<th>Rule</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>The suffix format cannot have more than four octets.</td>
<td>$4-$5 is invalid.</td>
</tr>
<tr>
<td>The octets must be in order.</td>
<td>-$2-$3-$4 is valid but -$3-$2-$4 is invalid.</td>
</tr>
<tr>
<td>Do not skip octets.</td>
<td>-$2-$3-$4 is valid but -$2-$4 is invalid.</td>
</tr>
<tr>
<td>Do not use a combination of both the $ and # symbols together as octet references; use only one of them.</td>
<td>-$2-$3-$4 is invalid.</td>
</tr>
<tr>
<td>The suffix format must contain at least the fourth octet. You must define at least one $ or #.</td>
<td>$4 is valid but $3 is invalid.</td>
</tr>
<tr>
<td>If the suffix format uses $ references, it cannot be preceded by a digit. You must add a non-digit prefix to each $ or # reference.</td>
<td>-$2-$3-$4</td>
</tr>
<tr>
<td>The \ character is the designated escape character for the $, # and \ characters. You cannot use the $ or # symbols as separators unless you prefix them with an escape character .</td>
<td>For the IP address 10.19.32.133, the format #-#1-#2-#3-#4 expands to -010-019-032-133.</td>
</tr>
<tr>
<td>The bulk host name format must comply with its zone host name policy.</td>
<td>You cannot insert a bulk host name format -?-$4 in a zone that uses Allow Underscore as host name policy because the policy does not allow you to use the ? character in the host name.</td>
</tr>
<tr>
<td>The bulk host name must comply with the maximum label length.</td>
<td>The sum of the bulk host name prefix and suffix cannot be greater than 63 characters. When you enter a suffix format, the NIOS appliance determines the length of the longest bulk host defined, and checks that the sum of the bulk host prefix and suffix length does not exceed 63 characters; if it does, an error message appears.</td>
</tr>
<tr>
<td>The bulk host name cannot result in an FQDN with more than 255 characters.</td>
<td>The NIOS appliance computes the maximum length of the bulk host suffix by expanding the bulk host IP format using 255.255.255.255. For the format string -$1-$2-$3-$4, the maximum length of the suffix is 255-255-255-255-255, that is, 16 characters. Therefore, the maximum length of the host prefix is 47 characters.</td>
</tr>
</tbody>
</table>
The bulk host name must not be the same as a CNAME/DNAME.

If there is a CNAME record with alias **foo-003-015**, you cannot insert a bulk host `foo/1.2.3.10/1.2.3.20` using template `$3-$4` because **foo-003-015** is also one of the synthetic host names in the bulk host.

Each host name in the bulk host must be unique.

You cannot insert a bulk host `foo/1.2.3.10/1.2.4.20` using the template `$4` because the system resolves the host name `foo-10` to both `1.2.3.10` and `1.2.4.10`. To ensure that the bulk host name is unique, use the template `$3-$4`.

You cannot insert a bulk host that violates the uniqueness of two bulk hosts that have the same prefix and use the same name format.

If there is a bulk host `foo/1.2.3.10/1.2.4.20` using the template `-3-$4`, you cannot insert another bulk host `foo/1.3.4.10/1.3.5.20` using the same template because the system resolves host name `foo-4-15` to both `1.2.4.15` and `1.3.4.15`. Instead, use the template `-2-$3-$4` to ensure that the two bulk hosts are unique.

The appliance provides four predefined formats. You can define additional formats or change the default format at the Grid level only. To define new bulk host name formats:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Grid DNS Properties**.
2. Select the **Host Naming** tab of the **Grid DNS Properties** editor.
   - The Bulk Host Name Formats table displays four predefined name suffix formats. The following examples show the host name that each format generates for the zone `test.com`:
     - Two Octets: `-3-$4`—Generates `foo-1-15.test.com`
     - One Octet: `$4`—Generates `foo-15.test.com`
     - For the IP address `10.100.0.10`, the format `-1$2-$3-$4` generates the host name suffix `10-100-0-10`.
   - The format `$1$2#$3#$4` generates the host name suffix `-010-100-000-010`.
3. Click **Add** to enter the name and format of a new bulk host name format.
4. Optionally, click the Default column of a format and select **Default** to make it the Grid default.
5. Save the configuration and click **Restart** if it appears at the top of the screen.

**Adding Bulk Hosts**

To add a bulk host:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Add -> Host -> Add Bulk Host**.
2. In the **Add Bulk Host** wizard, complete the following fields:
   - **Prefix**: If Grid Manager displays a zone name, enter a prefix (or series of characters) to insert at the beginning of each host name. The displayed zone name can either be the last selected zone or the zone from which you are adding the bulk host record. If no zone name is displayed or if you want to specify a different zone, click **Select Zone**. When there are multiple zones, Grid Manager displays the **Zone Selector** dialog box. Click a zone name in the dialog box, and enter a prefix for the bulk host record. You can enter any printable character that complies with the zone host name policy or you can also leave this blank. The sum of the bulk host prefix length and suffix length must not exceed 63 characters. When you enter a prefix, the NIOS appliance computes the maximum length of the bulk host suffix to verify that the total prefix and suffix length does not exceed 63 characters. If it does, the appliance displays an error message indicating the number of characters that you must remove to make a valid prefix.
     - **DNS View**: Displays the DNS view of the zone to which the bulk host records belong.
     - **Host Name Policy**: Displays the host name policy of the selected DNS zone.
     - **Name Format**: To override the default four-octet suffix format or the format set at the Grid level, and specify a different format, click **Override** and select a host name format from the **Name Formats** drop-down menu.
     - The **Name Formats** drop-down menu lists the formats **Four Octets**, **Three Octets**, **Two Octets**, and **One Octet** along with any other bulk host name formats that you have defined.
     - **Starting IP Address**: Enter the first IP address in the range of addresses for the group.
     - **End IP Address**: Enter the last IP address in the range of addresses for the group.
     - **Comment**: Optionally, enter additional information for this record.
     - **Automatically Add Reverse Mapping**: Click to have the appliance automatically create a PTR record for each IP address within the bulk host range.
     - **Disable**: Clear the check box to enable the record. Select the check box to disable it.
3. Click **Next** to define extensible attributes for the bulk host record. For information, see **Using Extensible Attributes**.
4. Save the configuration and click **Restart** if it appears at the top of the screen.

To modify or delete a bulk host, see **Modifying, Disabling, and Deleting Host and Resource Records**.

**Example 1 - Responding to DNS AXFR Queries**

This example shows the responses the bulk host `foo/1.2.3.10/1.2.3.20` returns to DNS AXFR (Full Zone Transfers) queries. If the bulk host uses the template `-3-$4`, the query returns:

```
foo-3-10.test.com foo-3-11.test.com
......
foo-3-20.test.com
```

Copyright ©2019, Infoblox, Inc. All right reserved.
If the bulk host uses the template `#2-#3-#4`, the query returns:

```
foo-002-003-010.test.com foo-002-003-011.test.com
......
foo-002-003-020.test.com
```

**Example 2 - Importing Zones with Bulk Hosts**

When you import zones with bulk hosts, the system selects the most specific match. The following example can possibly match three octet, two octet, and one octet formats; however, the system selects the most specific four octet default format.

The query:

```
foo-1-2-3-4 IN A 1.2.3.4
foo-1-2-3-5 IN A 1.2.3.5
```

Results in the match:

```
foo/1.2.3.4/1.2.3.5 (Four Octets)
Not in any of the following:
foo-1/1.2.3.4/1.2.3.5 (Three Octets) foo-1-2/1.2.3.4/1.2.3.5 (Two Octets) foo-1-2-3/1.2.3.4/1.2.3.5 (One Octet)
```

**Managing Resource Records**

DNS resource records provide information about objects and hosts. DNS servers use these records to respond to queries for hosts and objects. The appliance supports IDNs for all DNS resource records. For information about IDNs, see [Support for Internationalized Domain Names](#). Note that the appliance does not decode the IDN of a resource record to punycode. In other words, a record that contains a domain name in punycode is displayed in punycode and a record that contains an IDN is displayed in its native characters.

You can manage the following types of DNS resource records:

- **A (IPv4 Address)** — For information, see [Managing A Records](#).
- **NS (Name server)** — For information, see [Managing NS Records](#).
- **AAAA (IPv6 Address)** — For information, see [Managing AAAA Records](#).
- **PTR (Pointer)** — For information, see [Managing PTR Records](#).
- **MX (Mail exchanger)** — For information, see [Managing MX Records](#).
- **SRV (Service location)** — For information, see [Managing SRV Records](#).
- **TXT (Text)** — For information, see [Managing TXT Records](#).
- **TLSA (Transport Layer Security)** — For information, see [Managing TLSA Records](#).
- **CNAME ( Canonical name)** — For information, see [Managing CNAME Records](#).
- **DNAME** — For information, see [Managing DNAME Records](#).

**Managing A Records**

An A (address) record is a DNS resource record that maps a domain name to an IPv4 address. To define a specific name-to-address mapping, you can add an A record to a previously defined authoritative forward-mapping zone. If the zone is associated with one or more networks, the IP address must belong to one of the associated networks. For example, if the A record is in the corpxyz.com zone, which is associated with 10.1.0.0/16 network, then the IP addresses of the A record must belong to the 10.1.0.0/16 network. For information about associating zones and networks, see [Associating Networks with Zones](#).

The appliance also supports wildcard A records. For example, you can use a wildcard A record in the corpxyz.com domain to map queries for names such as www1.corpxyz.com, ftp.corpxyz.com, main.corpxyz.com, and so on to the IP address of a public-facing web server. Note that wildcard names only apply when the domain name being queried does not match any resource record.

NIOS allows superusers to add A records with a blank name. Limited-access users must have read/write permission to [Adding a blank A/AAAA record](#) to add A records with a blank name. You can assign global permission for specific admin groups and roles to allow limited-access users to add blank A records. For more information, see [Administrative Permissions for Adding Blank A or AAAA Records](#).

**Note:** If an A record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the **Name** field displays the record name in UTF-8 encoded format. For example, an A record with the domain name .test.com added through DDNS updates displays `\229\183\165\228\189\156\231\171\153.test.com` in the **Name** field.

**Adding A Records**

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Add -> Record -> Add A Record**.
2. In the **Add A Record** wizard, do the following:
   - **Name**: If Grid Manager displays a zone name, enter the hostname that you want to map to an IP address. The displayed zone name can either be the last selected zone or the zone from which you are adding the host record. If no zone name is displayed
or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Select dialog box. Click a zone name in the dialog box and then enter the hostname. The name you enter is prefixed to the DNS zone name that is displayed, and the complete name becomes the FQDN (fully qualified domain name) of the host. For example, if the zone name displayed is corp.xyz.com and you enter admin, then the FQDN becomes admin.corp.xyz.com. Ensure that the domain name you enter complies with the hostname restriction policy defined for the zone. To create a wildcard A record, enter an asterisk (*) in this field.

- **DNS View:** This field displays the DNS view to which the DNS zone belongs.
- **Shared Record Group:** This field appears only when you are creating a shared record. Click Select Shared Record Group. If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the Shared Record Group Selector dialog box. You can use filters or the Go to function to narrow down the list.
- **Hostname Policy:** Displays the hostname policy of the zone.
- **IP Addresses** section, click the Add icon and do one of the following:
  - Select Add Address to enter the IPv4 address to which you want the domain name to map, or
  - Select Next Available IPv4 to retrieve the next available IP address in a network.
- **Comment:** Optionally, enter additional information about the A record.
- **Create associated PTR record:** Select this option to automatically generate a PTR record that maps the specified IP address to the hostname. To create the PTR record, the reverse-mapping zone must be in the database.
- **Disable:** Select this check box to disable the record. Clear the check box to enable it.

3. Click **Next** to define extensible attributes. For information, see Using Extensible Attributes.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Modifying A Records

When you modify an A record, you can do the following:

- In the **General** tab, you can change the information you previously entered through the wizard, as described in Adding A Records.

- The **Discovered Data** tab displays discovered data, if any, for the record. For information, see Viewing Discovered Data.

You can also enter or edit information in the **TTL**, **Extensible Attributes** and **Permissions** tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.

### Managing NS Records

An NS record identifies an authoritative DNS server for a domain. Each authoritative DNS server must have an NS record. Grid Manager automatically creates NS records when you assign a Grid member as the primary server for a zone or when you assign an NS group to a zone. Grid Manager generates two NS records; an authoritative NS record for the current zone; and a delegation NS record for the parent zone for each name server available in the NS group. You cannot edit an automatically generated NS record. Note that when you delete a name server from an NS group, the NS record associated with the name server is deleted. For information about using NS Groups, see Importing Zone Data. You can manually create NS records for other zones. NS records associated with one or more IP addresses are used for related A record and PTR record generation. You can configure an NS record for anycast IP addresses on the appliance. For more information about anycast, see About Anycast Addressing for DNS.

### Adding NS Records

To add an NS record:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Add -> Record -> Add NS Record**.
2. In the **Add NS Record** wizard, complete the following fields:
   - **Zone:** The displayed zone name can either be the last selected zone or the zone from which you are adding the NS record. If no zone name is displayed or if you want to specify a different zone, click **Select Zone**.
   - **Hostname Policy:** Displays the hostname policy of the selected zone.
   - **Name Server:** Enter the host name that you want to configure as the name server for the zone. IDN is not supported in this field. You can use the punycode representation of an IDN in this field.

3. Click **Next** to enter IP addresses for the name server.
4. In the **Name Server Addresses** panel, click the Add icon and complete the following fields:
   - **Address:** Enter the IP address of the name server.
   - **Add PTR Record:** This field displays Yes by default, enabling the automatic generation of a PTR record for the IP address. You can select **No** to disable the generation of the PTR record.

5. Click **Next** to define extensible attributes, or save the configuration and click **Restart** if it appears at the top of the screen.
Modifying and Deleting NS Records

When you modify an NS record, you can change the following information:

- In the General tab, you can change the name server name.
- In the Addresses tab, you can do the following:
  - Delete an address by selecting it and clicking the Delete icon.
  - Add an address by clicking the Add icon, and then entering the IP address and completing the Add PTR Record field.

Managing AAAA Records

An AAAA (quad A address) record maps a domain name to an IPv6 address. To define a specific name-to-address mapping, add an AAAA record to a previously defined authoritative forward-mapping zone. If the zone is associated with one or more networks, the IP address must belong to one of the associated networks. For example, if the AAAA record is in the corpxyz.com zone, which is associated with the 1111:0001/32 network, then the IP addresses of the A record must belong to that network. For information about associating zones and networks, see Associating Networks with Zones.

Note: If an AAAA record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the Name field displays the record name in UTF-8 encoded format. For example, an AAAA record with the domain name .test.com added through DDNS updates displays 1229:183:165/228:189:156:231:171:153.test.com in the Name field.

NIOS allows superusers to add AAAA records with a blank name. Limited-access users must have read/write permission to Adding a blank A/A AAAA record to add AAAA records with a blank name. You can assign global permission for specific admin groups and roles to allow limited-access users to add blank AAAA records. For more information, see Administrative Permissions for Adding Blank A or AAAA Records.

Adding AAAA Records

To create an AAAA record:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add AAAA Record.
2. In the Add AAAA Record wizard, complete the following:
   - Name: If Grid Manager displays a zone name, enter the hostname that you want to map to an IP address. The displayed zone name can either be the last selected zone or the zone from which you are adding the AAAA record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter the hostname. The name you enter is prefixed to the DNS zone name that is displayed, and the complete name becomes the FQDN (fully qualified domain name) of the host. For example, if the zone name displayed is corpxyz.com and you enter admin, then the FQDN becomes admin.corpxyz.com.
   - DNS View: Displays the DNS view to which the selected DNS zone belongs.
   - Shared Record Group: This field appears only when you are creating a shared record. Click Select Shared Record Group. If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the Shared Record Group Selector dialog box. You can use filters or the Go to function to narrow down the list.
   - Hostname Policy: Displays the hostname policy of the zone.
   - IP Address: Enter the IPv6 address to which you want the domain name to map. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab:0:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered.
   - Comment: Optionally, enter additional information about this record.
   - Create associated PTR record: Select this option to automatically generate a PTR record that maps the specified IP address to the hostname. To create the PTR record, the reverse-mapping zone must be in the database.
   - Disable: Clear the check box to enable the record. Select the check box to disable it.
3. Click Next to define extensible attributes. For information, see Using Extensible Attributes.
4. Save the configuration and click Restart if it appears at the top of the screen.

Modifying AAAA Records

When you modify an AAAA record, you can do the following:

- In the General tab, you can change the information you previously entered through the wizard.
- In the Discovered Data tab, you can view discovered data, if any, for the record. For information, see Viewing Discovered Data.

You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.
Managing PTR Records

In a reverse-mapping zone, a PTR (pointer) record maps an IP address to a hostname. Before adding a PTR record to a reverse-mapping zone, you must first create the zone. You can also add PTR records to forward-mapping zones to support zerocnf (zero configuration networking), such as wide-area Bonjour. For information about the Bonjour protocol, refer to [http://www.apple.com/support/bonjour](http://www.apple.com/support/bonjour). Though adding PTR records to forward-mapping zones supports some of the use cases in RFC 1101, it does not support the network name mapping use case described in the RFC. For more information, refer to [http://tools.ietf.org/html/rfc1101](http://tools.ietf.org/html/rfc1101).

**Note:** If a PTR record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the Name and Domain Name fields display the record name in UTF-8 encoded format. For example, a PTR record with the domain name .test.com added through DDNS updates displays 229.183.165.228/189/156/231/171/153.test.com in the Name and Domain Name fields.

Adding PTR Records

To add a PTR record:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add PTR Record.
2. In the Add PTR Record wizard, do the following:
   - **Name or IP Address:** From the drop-down list, select Name or IP Address. When you select Name, click Select Zone to select a zone, and then enter a value for the PTR record. When you are adding a PTR record to a reverse-mapping zone, you can enter a value from 0 to 255 in the Name or IP Address field. Note that when you launch this wizard from the IPAM tab, you can only select a reverse-mapping zone. When you launch this from a reverse-mapping zone, the IP address field is populated with the prefix that corresponds to the selected zone. When you launch this from a forward-mapping zone, you can only specify the host name, not an IP address.
   - **When you select IP Address,** enter the IPv4 or IPv6 address that you want to map to the domain name.
   - **DNS View:** If you entered an IP address, you must select the DNS view of the PTR record. If you entered a name, this field displays the DNS view of the selected zone.
   - **Domain Name:** Enter the domain name to which you want the PTR record to point. For example, you can enter corpxyz.com.
   - **Comment:** Optionally, enter information about the PTR record.
   - **Disable:** Select this check box to disable the record. Clear the check box to enable it.
3. Save the configuration, or click Next to define extensible attributes. For information, see [Using Extensible Attributes](#).
4. Click Restart if it appears at the top of the screen.

To schedule this task, click the Schedule icon at the top of the wizard. In the Schedule Change panel, click Later, and then specify a date, time, and time zone.

**Note:** When you add a PTR record to a forward-mapping zone, a message may appear on the top of the wizard if a Grid member is configured to ignore DNS queries for PTR records in forward-mapping zones. Contact Infoblox Technical Support for more information about this message.

Modifying PTR Records

Do the following to modify a PTR record:

- In the General tab, you can change the information you previously entered through the wizard. Note that you cannot change an IPv4 address to an IPv6 address or move a PTR record from a forward-mapping zone to a reverse-mapping zone and vice versa. When you modify a PTR record that belongs to a forward-mapping zone, you can only modify the name since there is no IP address for such record. For information, see [Adding PTR Records](#).
- In the Discovered Data tab, you can view discovered data, if any, for the record. For information, see [Viewing Discovered Data](#).

You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see [Modifying, Disabling, and Deleting Host and Resource Records](#).

Managing MX Records

An MX (mail exchanger) record maps a domain name to a mail exchanger. A mail exchanger is a server that either delivers or forwards mail. You can specify one or more mail exchangers for a zone, as well as the preference for using each mail exchanger. A standard MX record applies to a particular domain or subdomain.

You can use a wildcard MX record to forward mail to one mail exchanger. For example, you can use a wildcard MX record in the corpxyz.com domain to forward mail for eng.corpxyz.com and sales.corpxyz.com to the same mail exchange, as long as the domain names do not have any matching resource record. Wildcards only apply when the domain name being queried does not match any record.

**Note:** If an MX record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the Mail Destination a
Mail Exchanger fields display the record name in UTF-8 encoded format. For example, an MX record with the domain name .test.com added through DDNS updates displays `229\183\165\228\189\156\231\171\153.test.com` in the Mail Destination and Mail Exchanger fields.

See Figure 20.1.

Figure 20.1 MX Records

The following MX records ...
... direct queries for one or more domains ...
... to the same mail exchanger:

An MX record for the mail exchanger that answers queries for just the corpxyz.com domain (and its corresponding A record):

```
corpxyz.com IN MX 0 mail1.corpxyz.com
mail1.corpxyz.com IN A 10.2.2.10
```

An MX record for just site1.corpxyz.com, a subdomain of corpxyz.com:

```
site1.corpxyz.com IN MX 0
mail1.corpxyz.com
```

A wildcard MX record for the corpxyz.com domain:

```
*corpxyz.com IN MX 0 mail1.corpxyz.com
```

**Note:** You must also create an A record for the host defined as a mail exchanger in an MX record.

Adding MX Records

To add an MX record from the Tasks Dashboard, see Add MX Record. You can also add MX records from the Data Management tab -> DNS tab by clicking Add -> Record -> Add MX Record from the Toolbar.

Modifying and Deleting MX Records

When you modify an MX record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.

Managing SRV Records

An SRV (service location) record directs queries to hosts that provide specific services. For example, if you have an FTP server, then you might create an SRV record that specifies the host which provides the service. You can specify more than one SRV record for a host. For more information about SRV records, see RFC 2052, A DNS RR for specifying the location of services (DNS SRV).

**Note:** If an SRV record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the Name and SRV Target fields display the domain name in UTF-8 encoded format. For example, an SRV record with the domain name .test.com added through DDNS updates displays `231\148\181\232\132\145.test.com` in the Name and SRV Target fields.

Adding SRV Records

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add SRV Record.
2. In the Add SRV Record wizard, complete the following fields:
   - **Display input as:** Select the format in which you want the SRV record to be displayed. When you select RFC 2782 format, the appliance follows the `_service._protocol.name` format as defined in RFC 2782. When you select Free format, enter the entire name in the Domain field.
   - **Service:** Specify the service that the host provides. You can either select a service from the list or type in a service, if it is not on the list. For example, if you are creating a record for a host that provides FTP service, select ftp. To distinguish the service name labels from the domain name, the service name is prefixed with an underscore. If the name of the service is defined at [http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml](http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml), use that name. Otherwise, you can use a locally-defined name.
• **Protocol:** Specify the protocol that the host uses. You can either select a protocol from the list or type in a protocol, if it is not on the list. For example, if it uses TCP, select _tcp. To distinguish the protocol name labels from the domain name, the protocol name is prefixed with an underscore.

• **Domain:** If Grid Manager displays a zone name, enter the name here to define an SRV record for a host or subdomain. The displayed zone name can either be the last selected zone or the zone from which you are adding the SRV record. If no zone name is displayed or if you want to specify a different zone, click **Select Zone.** When there are multiple zones, Grid Manager displays the **Zone Selector** dialog box. Click a zone name in the dialog box, and then enter the name to define the SRV record. The NIOS appliance prefixes the name you enter to the domain name of the selected zone. For example, if you want to create an SRV record for a web server whose host name is www2.corpxyz.com and you define the SRV record in the corpxyz.com zone, enter www2 in this field. To define an SRV record for a domain whose name matches the selected zone, leave this field blank. The NIOS appliance automatically adds the domain name (the same as the zone name) to the SRV record. For example, if you want to create an SRV record for the corpxyz.com domain and you selected the corpxyz.com zone, leave this field blank.

• **Preview:** After you have entered all the information, this field displays the FQDN, which is the concatenation of the Service, Protocol, and Domain fields.

• **Shared Record Group:** This field appears only when you are creating a shared record. Click **Select Shared Record Group.** If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the **Shared Record Group Selector** dialog box. You can use filters or the Go to function to narrow down the list.

• **Priority:** Select or enter an integer from 0 to 65535. The priority determines the order in which a client attempts to contact the target host; the domain name host with the lowest number has the highest priority and is queried first. Target hosts with the same priority are attempted in the order defined in the **Weight** field.

• **Weight:** Select or enter an integer from 0 to 65535. The weight allows you to distribute the load between target hosts. The higher the number, the more that host handles the load (compared to other target hosts). Larger weights give a target host a proportionately higher probability of being selected.

• **Port:** Specify the appropriate port number for the service running on the target host. You can use standard or nonstandard port numbers, depending on the requirements of your network. You can select a port number from the list or enter an integer from 0 to 65535.

• **Target:** Enter the canonical domain name of the host (not an alias); for example, www2.corpxyz.com to 65535.

**Note:** In addition, you need to define an A record mapping the canonical name of the host to its IP address.

• **Comment:** Enter a descriptive comment for the record.

• **Disable:** Clear the check box to enable the record. Select the check box to disable it.

3. Save the configuration, or click **Next** to define extensible attributes. For information, see Using Extensible Attributes.

4. Click **Restart** if it appears at the top of the screen.

### Modifying and Deleting SRV Records

Do the following to modify an SRV record:

- In the **General** tab, the **Display input as** field displays the format in which the SRV record was configured. For RFC 2782 format, the appliance matches the \(service.protocol.name\) format and displays the corresponding information in the Service and Protocol fields. If the appliance cannot match the service and protocol, it displays the entire name in the Domain field. For Free format, the entire name is displayed in the Domain field. For more information about the other fields, see Adding SRV Records.

**Note:** The appliance does not match the service and protocol names to exactly how they appear in the drop-down lists. It only checks whether the first two parts of the names start with an underscore. If the first two parts do not start with an underscore, the appliance assumes it is a free format. For example, _abc._xyz.name is considered as RFC 2782 format even though _abc is not in the Service drop-down list, and _xyz is not in the Protocol drop-down list. Grid Manger displays _abc in the **Service** field and _xyz in the **Protocol** field. On the other hand, “abc.xyz.name” is considered as a free format because the first two parts do not start with underscores, and Grid Manager displays this in its entirety in the Domain field.

You can also enter or edit information in the **TTL**, **Extensible Attributes**, and **Permissions** tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.

### Managing TXT Records

A **TXT** (text record) record contains supplemental information for a host. For example, if you have a sales server that serves only North America, you can create a text record stating this fact. You can create more than one text record for a domain name.

**Note:** If a TXT record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the **Name** field displays the domain name in UTF-8 encoded format. For example, a TXT record with the domain name .test.com added through DDNS updates displays values:148181232:132145.test.com in the **Name** field.

### Using TXT Records for SPF
SPF (Sender Policy Framework) is an anti-forgery mechanism designed to identify spam e-mail. SPF fights e-mail address forgery and makes it easier to identify spam, worms, and viruses. Domain owners identify sending mail servers in DNS. SMTP receivers verify the envelope sender address against this information, and can distinguish legitimate mail from spam before any message data is transmitted.

SPF makes it easy for a domain to say, “I only send mail from these machines. If any other machine claims that I’m sending mail from there, they’re not valid.” For example, when an AOL user sends mail to you, an email server that belongs to AOL connects to an email server that belongs to you. AOL uses SPF to publish the addresses of its email servers. When the message comes in, your email servers can tell if the server that sent the email belongs to AOL or not.

You can use TXT records to store SPF data that identifies what machines send mail from a domain. You can think of these specialized TXT records as reverse MX records that e-mail servers can use to verify if a machine is a legitimate sender of an e-mail.

**SPF Record Examples**

corpxyz.com. IN TXT "v=spf1 mx -all"
corpxyz.net. IN TXT "v=spf1 a:mail.corpxyz.com -all" corpxyz.net. IN TXT "v=spf1 include:corpxyz.com -all" corpxyz.net. IN TXT "v=spf1 include:corp200.com -all"

**Adding TXT Records**

To add an TXT record from the Tasks Dashboard, see Add TXT Record. You can also add TXT records from the Data Management tab -> DNS tab by clicking Add -> Record -> Add TXT Record from the Toolbar.

**Modifying and Deleting TXT Records**

When you modify a TXT record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.

**Managing TLSA Records**

A TLSA record is used to associate a TLS (Transport Layer Security) server certificate or a public key with a domain name. For example, you can define whether a certificate or a public key must be associated with a domain name when you define a TLSA resource record through Grid Manager. When you define your own TLSA record, you do not have to depend on an external Certificate Authority to issue a digitally signed TLS certificate for your domain name. When a client queries the domain name, TLSA records are matched to authenticate associated TLS certificates.

**Using TLSA Records for DANE**

Infoblox supports DANE (DNS-based Authentication of Named Entities) protocol to secure information about domain names. DANE uses DNSSEC to sign certificates and keys that are used by the TLS and distributes secure information about the domain name using DNS. With DANE, you can make an authoritative binding between the domain name and a certificate or a public key, whichever is used by a host for the respective domain. You can define what kind of certificates or public keys must be associated with a domain name to prevent vulnerability attacks and to reduce or prevent the interaction of third party Certification Authorities to issue PKIX certificates. For detailed information about the TLSA record format and certificate usage, refer to RFC 6698 The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA.

**Note:** You can add a TLSA record to a DNSSEC signed zone only. You cannot unsign a zone that contains a TLSA record.

**Adding TLSA Records**

To add a TLSA record:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> TLSA Record.
2. In the Add TLSA Record wizard, complete the following fields:
   - **Display input as**: Select either Strict format (._port._protocol.domain) or Free format. Grid Manager selects Strict format by default. In this format, you can choose port and protocol values from the list. When you select Free format, you cannot specify these values.
   - **Port**: Select a value from the drop-down list to indicate the port on which the TLS-based service is active. The values in the drop-down list are:
     - 21 (FTP)
     - 22 (SSH)
     - 23 (Telnet)
     - 25 (SMTP)
     - 80 (HTTP)
     - 88 (Kerberos)
• 389 (LDAP)
• 443 (HTTPS)
• 464 (KPASSWD)
• 3268 (GC)

- **Protocol**: Select a value from the drop-down list to indicate the protocol that is used for secure communication. The values in the drop-down list are:
  - _msdcs
  - _sites
  - _tcp
  - _udp

**Note**: When you select **Strict format**, **Port** and **Protocol** values are set to 443 (HTTPS) and _tcp, by default. You can change these values. When you select **Free format**, you cannot edit the mentioned values.

- **Name**: Enter a name for the TLSA resource record. You can specify a name only when you select **Free format**.
- **Select Zone**: Click to select a zone. You can only select signed zones to associate with a TLSA resource record. For more information, see **Signing a Zone**. Click **Clear** to clear the **Name** that you have entered.
- **FQDN**: This is displayed by default. You cannot modify the value. TLSA resource records are stored using the domain name that you select. When you select **Free format**, **name.domain** is displayed as the FQDN. Example: abc.example.com. When you select **Strict format**, _port_.protocol.domain is displayed as the FQDN, where:
  - _port_ indicates the port on which the TLS-based service is active.
- **Protocol** to _tcp, which indicates that the HTTP server is running TLS on port 443. To request TLSA record for **www.example.com**, you must use _443_.tcp. www.example.com. Similarly, to request a TLSA resource record for an SMTP server running the STARTTLS protocol on port 25 at mail.example.com, you must use _25_.tcp.mail.example.com.
- **DNS View**: The DNS View associated with the selected DNS zone is displayed.
- **Certificate Usage**: Select a value from the drop-down list to indicate how the certificate or the public key associated with the domain name is matched when the client queries for the domain name on the TLS server. The values in the drop-down list are: _PKIX-TA_, _PKIX-EE_, _DANE-TA_, and _DANE-EE_.
  - With _PKIX-TA_ and _PKIX-EE_, you need additional Trust Anchors to validate peer certificate chains. These Trust Anchors must be mutually trusted by both the TLS server and the client. For more information, refer to RFC 6968 The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA.
  - When you select _DANE-TA_ and _DANE-EE_, the TLSA records that you define using Grid Manager are sufficient to verify the client's certificate chain and additional Trust Anchors are not required to authenticate the public key or certificate data. For more information, refer to RFC 6968 The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA.
- **Selector**: Select a value from the drop-down list to indicate whether you are associating an entire certificate or only the public key with the domain. When you select a value, it indicates which part of the TLS certificate presented by the server is matched with the associated data. The values in the drop-down list are **Full certificate** and **Subject Public Key Info**. NIOS builds an hexadecimal format for the entire certificate when you select **Full certificate**. If you select **Subject Public Key Info**, NIOS extracts the public key and builds a hexadecimal format for it.
  - **Matched Type**: Select a value from the drop-down list to indicate how a TLS certificate or the public key of the domain received from the client must be matched with the certificate or the certificate key that you have specified for the respective domain in the TLS server. You can select to match the entire content or only the hash of the selector. The values in the drop-down list are: **No hash**, **SHA 256 bit**, and **SHA 512 bit**. If you select **No hash**, the TLS server performs an exact match on the selected content. When you select either **SHA 256 bit** or **SHA 512 bit**, only the hash of the selected content is matched by the TLS server.
- **Certificate Data**: Enter the certificate data that must be matched for authentication. You can either paste the full certificate or the corresponding public key when the **Matched Type** is set to **No hash**. Based on the values that you select for the **Selector** and the **Matched Type**, the server builds a hexadecimal format for the TLSA record. If you set the **Matched Type** to **SHA 256 bit** or **SHA 512 bit**, you must specify only the hash of the full certificate or the public key.
- **Get From File**: Click this to upload the certificate or the public key to the server. Note the following:
  - When you select **Strict format**, you must provide either the certificate or public key or hash of any of them. The value must be based on the **Selector** and **Matched Type** field values.
  - When you select **Free format**, you must upload the certificate in DER format. The server builds an appropriate hexadecimal format for the TLSA record based on the **Selector** value.
- **Comment**: Optionally, enter a descriptive comment for the TLSA record.
- **Disable**: Clear the check box to enable the record. Select the check box to disable it.

**Note**: You cannot add TLSA resource records during a scheduled full upgrade from an earlier NIOS version to 8.0 and later. Grid Manager will not convert a TLSA resource record that is stored in **bind_resource_record** during an upgrade. You must do it manually after an upgrade.

You can also do the following:

- Use **Global Search** to search for TLSA records. For information, see **Global Search**.
- Use **Copy Records** to copy TLSA records between DNS zones. For information, see **Copying Zone Records**.
- Define global permission for **All TLSA records** with read-only, read/write or deny access. You can also define object level permission for

Unknown macro: `html`
Modifying and Deleting TLSA Records

When you modify a TLSA record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.

Managing CNAME Records

A CNAME record maps an alias to a canonical name. You can use CNAME records in both forward- and IPv4 reverse-mapping zones to serve two different purposes. (At this time, you cannot use CNAME records with IPv6 reverse-mapping zones.)

Note: If a CNAME record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the Alias and Canonical Name fields display the domain name in UTF-8 encoded format. For example, a CNAME record with the domain name .test.com added through DDNS updates displays \231\148\181\232\132\145.test.com in the Canonical Name and Alias fields.

CNAME Records in Forward-Mapping Zones

In a forward-mapping zone, a CNAME record maps an alias to a canonical (or official) name. CNAME records are often more convenient to use than canonical names because they can be shorter or more descriptive. For example, you can add a CNAME record that maps the alias qa.engr to the canonical name qa.engr.corpxyz.com.

Note: A CNAME record does not have to be in the same zone as the canonical name to which it maps. In addition, a CNAME record cannot have the same name as any other record in that zone.

To add a CNAME record to a forward-mapping zone from the Tasks Dashboard, see Add CNAME Record. You can also add CNAME records from the Data Management tab -> DNS tab by clicking Add -> Record -> Add CNAME Record from the Toolbar.

CNAME Records in IPv4 Reverse-Mapping Zones

You can add CNAME records to an IPv4 reverse-mapping zone to create aliases to addresses maintained by a different name server when the reverse-mapping zone on the server is a delegated child zone with fewer than 256 addresses. This technique allows you to delegate responsibility for a reverse-mapping zone with an address space of fewer than 256 addresses to another authoritative name server. See Figure 20.2 and RFC 2317, Classless IN-ADDR.ARPA delegation.

Figure 20.2 CNAME Records in a Reverse-Mapping Zone
You add CNAME records in the parent zone on your name server. The aliases defined in those CNAME records point to the addresses in PTR records in the child zone delegated to the other server.

When you define a reverse-mapping zone that has a netmask from /25 (255.255.255.128) to /31 (255.255.255.254), you must include an RFC 2317 prefix. This prefix can be anything, from the address range (examples: 0-127, 0/127) to descriptions (examples: first-network, customer1).

On a NIOS appliance, creating such a reverse-mapping zone automatically generates all the necessary CNAME records. However, if you need to add them manually to a parent zone that has a child zone with fewer than 255 addresses.

**Adding CNAME Records**

To add a CNAME record to a forward-mapping or reverse-mapping zone from the Tasks Dashboard, see Add CNAME Record. You can also add CNAME records from the Data Management tab -> DNS tab by clicking Add -> Record -> Add CNAME Record from the Toolbar.

**Modifying and Deleting CNAME Records**

When you modify a CNAME record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.

**Managing DNAME Records**

A DNAME record maps all the names in one domain to those in another domain, essentially substituting one domain name suffix with the other (see RFC 2672, Non-Terminal DNS Name Redirection). For example, adding a DNAME record to the corpxyz.com domain mapping "corpxyz.com" to "corp200.com" maps name-x.corpxyz.com to name-x.corp200.com:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Target Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>server1.corpxyz.com</td>
<td>server1.corp200.com</td>
</tr>
</tbody>
</table>
server2.corpxyz.com —> server2.corp200.com
server3.corpxyz.com —> server3.corp200.com
....corpxyz.com —> ....corp200.com

Note: If a DNAME record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the Alias and Target fields display the domain name in UTF-8 encoded format. For example, a DNAME record with the domain name .test.com added through DDNS updates displays \231\148\181\232\132\145.test.com in the Alias and Target fields.

When a request arrives for a domain name to which a DNAME record applies, the NIOS appliance responds with a CNAME record that it dynamically creates based on the DNAME definition. For example, if there is a DNAME record

corpxyz.com.
DNAME

and a request arrives for server1.corpxyz.com, the NIOS appliance responds with the following CNAME record:

server1.corpxyz.com.
CNAME

If responding to a name server running BIND 9.0.0 or later, the NIOS appliance also includes the DNAME record in its response, so that name server can also create its own CNAME records based on the cached DNAME definition.

The following are two common scenarios for using DNAME records:

- One company buys another and wants people using both the old and new name spaces to reach the same hosts.
- A virtual Web hosting operation offers different "vanity" domain names that point to the same server or servers.

There are some restrictions that apply to the use of DNAME records:

- You cannot have a CNAME record and a DNAME record for the same subdomain.
- You cannot use a DNAME record for a domain or subdomain that contains any subdomains. You can only map the lowest level subdomains (those that do not have any subdomains below them). For an example of using DNAME records in a multi-tiered domain structure, see Figure 20.3.

Figure 20.3 Adding DNAME Records for the Lowest Level Subdomains

In the case of a domain structure consisting of a single domain (no subdomains), adding a DNAME record redirects queries for every name in the domain to the target domain, as shown in Figure 20.4.

Figure 20.4 Adding a DNAME Record for a Single Domain

Copyright ©2019, Infoblox, Inc. All right reserved.
When using a DNAME record, you must copy the resource records for the source domain to the zone containing the target domain, so that the DNS server providing service for the target domain can respond to the redirected queries.

Copy from `corpxyz.com` to `corpxyz.corp200.com`

<table>
<thead>
<tr>
<th>Resource</th>
<th>Source Zone</th>
<th>Target Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>www1 A</td>
<td>10.1.1.10</td>
<td>10.1.1.10</td>
</tr>
<tr>
<td>www2 A</td>
<td>10.1.1.11</td>
<td>10.1.1.11</td>
</tr>
<tr>
<td>ftp1 A</td>
<td>10.1.1.20</td>
<td>10.1.1.20</td>
</tr>
<tr>
<td>mail1 A</td>
<td>10.1.1.30</td>
<td>10.1.1.30</td>
</tr>
</tbody>
</table>

After copying these records to the zone containing the `corpxyz.corp200.com` domain, delete them from the zone containing the `corpxyz.com` domain.

If DNS service for the source and target domain names is on different name servers, you can import the zone data from the NIOS appliance hosting the source domain to the appliance hosting the target domain. For information about this procedure, see Importing Zone Data.

If DNS service for the source and target domain names is on the same name server and the parent for the target domain is on a different server, you can delegate DNS services for the target domain name to the name server that provided—and continues to provide—DNS service for the source domain name (see Figure 20.5). By doing this, you can continue to maintain resource records on the same server, potentially simplifying the continuation of DNS administration.

Figure 20.5 Making the Target Zone a Delegated Zone

Note: This is a conceptual representation of domain name mapping and depicts the resulting hierarchical relationship of corp200.com as the parent zone for corpxyz.corp200.com. The hosts are not physically relocated.
Note: This is a conceptual representation of domain name mapping and depicts the resulting hierarchical relationship of corp200.com as the parent zone for corpxyz.corp200.com. The hosts are not physically relocated.

The following tasks walk you through configuring the two appliances in Figure 20.5 to redirect queries for corpxyz.com to corpxyz.corp200.com using a DNAME record:

On the ns1.corpxyz.com name server, do the following:

2. Copy all the resource records for the domain or subdomain to which the DNAME record is going to apply from corpxyz.com to corpxyz.corp200.com.

   Note: Because you can only specify the records by type, not individually, you might have to copy some records that you do not want and then delete them from the corpxyz.corp200.com zone.

3. In the corpxyz.com zone, delete all the resource records for the domain or subdomain to which the DNAME record is going to apply.
4. Add a DNAME record to the corpxyz.com zone specifying "corpxyz.com" as the domain and "corpxyz.corp200.com" as the target domain.
5. On the ns1.corp200.com name server, add corpxyz.corp200.com as a delegated zone and specify ns1.corpxyz.com as the name server for it. See Configuring a Delegation.

DNAME Records for Forward-Mapping Zones

To add a DNAME record to a forward-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add DNAME Record.
2. In the Add DNAME Record wizard, complete the following fields:

   • Alias: If Grid Manager displays a zone name, enter the name of a subdomain here. If you are adding a DNAME record for the entire zone, leave this field empty. This field is for adding a DNAME record for a subdomain within the selected zone. The displayed zone name can either be the last selected zone or the zone from which you are adding the DNAME record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter the name of a subdomain.
   • Target: Enter the domain name to which you want to map all the domain names specified in the Alias field.
   • Comment: Enter identifying text for this record, such as a meaningful note or reminder.
   • Disable: Clear the check box to enable the record. Select the check box to disable it.

3. Save the configuration, or click Next to define extensible attributes. For information, see Using Extensible Attributes.
4. Click Restart if it appears at the top of the screen.

DNAME Records for Reverse-Mapping Zones

You can use DNAME records to redirect reverse lookups from one reverse-mapping zone to another. You can use DNAME records for reverse-mapping zones to simplify the management of subzones for classless address spaces larger than a class C subnet (a subnet with a 24-bit netmask).

RFC 2672, Non-Terminal DNS Name Redirection, includes an example showing the delegation of a subzone for an address space with a 22-bit netmask inside a zone for a larger space with a 16-bit netmask:

$ORIGIN 0.192.in-addr.arpa.

<table>
<thead>
<tr>
<th>8/22</th>
<th>NS</th>
<th>ns.slash-22-holder.example.</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>DNAME</td>
<td>8.8/22</td>
</tr>
<tr>
<td>9</td>
<td>DNAME</td>
<td>9.8/22</td>
</tr>
<tr>
<td>10</td>
<td>DNAME</td>
<td>10.8/22</td>
</tr>
<tr>
<td>11</td>
<td>DNAME</td>
<td>11.8/22</td>
</tr>
</tbody>
</table>

The reverse-mapping zone 0.192.in-addr.arpa. applies to the address space 192.0.0.0/16. Within this zone is a subzone and subdomain with the abbreviated name 8/22. (Its full name is 8/22.0.192.in-addr.arpa.) This subdomain contains its own subdomains corresponding to the 1024 addresses in the 192.0.8.0/22 subnet:

• Subdomain 8/22 (8/22.0.192.in-addr.arpa)
Subdomain 8.8/22 for addresses 192.0.8.0 – 192.0.8.255 (or 192.0.8.0/24)
Subdomain 9.8/22 for addresses 192.0.9.0 – 192.0.9.255 (or 192.0.9.0/24)
Subdomain 10.8/22 for addresses 192.0.10.0 – 192.0.10.255 (or 192.0.10.0/24)
Subdomain 11.8/22 for addresses 192.0.11.0 – 192.0.11.255 (or 192.0.11.0/24)

The NS record delegates authority for the reverse-mapping subzone 8/22 to the DNS server ns.slash-22-holder.example. Finally, the DNAME records provide aliases mapping domain names that correspond to the 192.0.8.0/24, 192.0.9.0/24, 192.0.10.0/24, and 192.0.11.0/24 subnets to the respective subdomains 8.8/22, 9.8/22, 10.8/22, and 11.8/22 in the 8/22.0.192.in-addr.arpa subzone.

Note: NIOS appliances support DNAME records in reverse-mapping zones that map addresses to target zones with a classless address space larger than a class C subnet. However, NIOS appliances do not support such target zones.

You might also use DNAME records if you have a number of multihomed appliances whose IP addresses must be mapped to a single set of domain names. An example of this is shown in Figure 20.6.

Figure 20.6 DNAME Records to Simplify DNS for Multihomed Appliances

Note: If you specify a subdomain in the Domain Name field when configuring a DNAME record, and the subdomain is also a subzone, the DNAME record appears in the list view for the subzone, not in the list view for the parent zone that was selected when adding it.

To add a DNAME record to a reverse-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add DNAME Record.
2. In the Add DNAME Record wizard, complete the following fields:
   - **Alias**: If Grid Manager displays a zone name, enter the name of a subdomain here. If you are adding a DNAME record for the entire zone, leave this field empty. This field is for adding a DNAME record for a subdomain within the selected zone. The displayed zone name can either be the last selected zone or the zone from which you are adding the CNAME record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter the name of a subdomain.
   - **Target**: Type the name of the reverse-mapping zone to which you want to map all the addresses specified in the Domain Name field.
   - **Comments**: Enter identifying text for this record, such as a meaningful note or reminder.
   - **Disable**: Clear the check box to enable the record. Select the check box to disable it.
3. Save the configuration, or click Next to define extensible attributes. For information, see Using Extensible Attributes.
4. Click Restart if it appears at the top of the screen.
Modifying and Deleting DNAME Records

When you modify a CNAME record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.

Managing NAPTR Records

A NAPTR (Name Authority Pointer) record specifies a rule that uses a substitution expression to rewrite a string into a domain name or URI (Uniform Resource Identifier). A URI is either a URL (Uniform Resource Locator) or URN (Uniform Resource Name) that identifies a resource on the Internet.

NAPTR records are usually used to map E.164 numbers to URIs or IP addresses. An E.164 number is a telephone number, 1-555-123-4567 for example, in a format that begins with a country code, followed by a national destination code and a subscriber number. (E.164 is an international telephone numbering system recommended by the International Telecommunication Union.) Thus, NAPTR records allow us to use telephone numbers to reach devices, such as fax machines and VoIP phones, on the Internet.

To map an E.164 to a URI, the E.164 number must first be transformed into a domain name. ENUM (E.164 Number Mapping) specifies a method for converting E.164 numbers to domain names. For example, using the method specified by ENUM, the telephone number 1-555-123-4567 becomes the domain name 7.6.5.4.3.2.1.5.5.5.1.e164.arpa. For details about ENUM, refer to RFC 3761, The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM).

After the E.164 number is converted to a domain name, a DNS client can then perform a DNS lookup for the NAPTR records of the domain name. The following example illustrates how a DNS client processes NAPTR records.

In this example, the telephone number 1-555-123-4567 is converted to the domain name 7.6.5.4.3.2.1.5.5.5.1.e164.arpa. The DNS client then sends a query to the Infoblox DNS server for the NAPTR records associated with 7.6.5.4.3.2.1.5.5.5.1.e164.arpa. The Infoblox DNS server returns the following NAPTR record:

```
$ORIGIN 7.6.5.4.3.2.1.5.5.5.1.e164.arpa
IN NAPTR 10 100 "U" "sip + E12U" "!.*$!sip:jdoe@corpxyz.com!" .
```

<table>
<thead>
<tr>
<th>Order</th>
<th>Preference</th>
<th>Flag</th>
<th>Service</th>
<th>Regular Expression</th>
<th>Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>U</td>
<td></td>
<td>!.*$!sip:<a href="mailto:jdoe@corpxyz.com">jdoe@corpxyz.com</a>!</td>
<td></td>
</tr>
</tbody>
</table>

The DNS client then examines the fields in the NAPTR record as follows:

- If a DNS client receives multiple NAPTR records for a domain name, the value in the Order field determines which record is processed first. It processes the record with the lowest value first.
- The DNS client uses the Preference value when the Order values are the same. Similar to the Preference field in MX records, this value indicates which NAPTR record the DNS client should process first when the records have the same Order value. It processes the record with the lowest value first.
- In the example, the DNS client ignores the Order and Preference values because it received only one NAPTR record.
- The Flag field indicates whether the current lookup is terminal; that is, the current NAPTR record is the last NAPTR record for the lookup. It also provides information about the next step in the lookup process. The flags that are currently used are:
  - U: Indicates that the output maps to a URI (Uniform Record Identifier).
  - S: Indicates that the output is a domain name that has at least one SRV record. The DNS client must then send a query for the SRV record of the resulting domain name.
  - A: Indicates that the output is a domain name that has at least one A or AAAA record. The DNS client must then send a query for the A or AAAA record of the resulting domain name.
  - P: Indicates that the protocol specified in the Service field defines the next step or phase.
- If the Flag field is blank, this indicates that the client must use the resulting domain name to look up other NAPTR records.
- The Service field specifies the service and protocol that are used to communicate with the host at the domain name. In the example, the service field specifies that SIP (Session Initiation Protocol) is used to contact the telephone service.
- The regular expression specifies the substitution expression that is applied to the original string of the client. In the example, the regular expression `!.*$!sip:jdoe@corpxyz.com!` specifies that the domain name 7.6.5.4.3.2.1.5.5.5.1.e164.arpa is replaced with `sip:jdoe@corpxyz.com`.
  
The regular expression in a NAPTR record is always applied to the original string of the client. It must not be applied to a domain name that resulted from a previous NAPTR rewrite.
• The Replacement field specifies the FQDN for the next lookup, if it was not specified in the regular expression.

Note: If a NAPTR record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the Domain and Replacement fields display the domain name in UTF-8 encoded format. For example, a NAPTR record with the domain name .test.com added through DDNS updates displays 231/148/181/232/132/145.test.com in the Domain and Replacement fields.

Adding NAPTR Records

To add a NAPTR record:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add NAPTR Record.
2. In the Add NAPTR Record wizard, complete the following fields:
   • Domain: If Grid Manager displays a zone name, enter the domain name to which this resource record refers. The displayed zone name can either be the last selected zone or the zone from which you are adding the NAPTR record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter a domain name for the record. The name you enter is prefixed to the DNS zone name that is displayed, and the complete name becomes the FQDN (fully qualified domain name) of the record. For example, if the zone name displayed is corpxyz.com and you enter admin, then the FQDN becomes admin.corpxyz.com. This field is not displayed when you configure a NAPTR record for a DTC server.
   • DNS View: Displays the DNS view of the selected zone.
   • Service: Specifies the service and protocol used to reach the domain name that results from applying the regular expression or replacement. You can enter a service or select a service from the list.
   • Flags: The flag indicates whether the resulting domain name is the endpoint URI or if it points to another record. Select one of the following:
     U: Indicates that the output maps to a URI.
     S: Indicates that the resulting domain name has at least one SRV record.
     A: Indicates that the resulting domain name has at least one A or AAAA record.
     P: Indicates that this record contains information specific to another application.
   • Order: Select an Integer from 10 to 100, or enter a value from 0 to 65535. This value indicates the order in which the NAPTR records must be processed. The record with the lowest value is processed first.
   • Preference: Select an Integer from 10 to 100, or enter a value from 0 to 65535. Similar to the Preference field in MX records, this value indicates which NAPTR record should be processed first when the records have the same Order value. The record with the lowest value is processed first.
   • REGEX: The regular expression that is used to rewrite the original string from the client into a domain name. RFC 2915 specifies the syntax of the regular expression. Note that the appliance validates the regular expression syntax between the first and second delimiter against the Python re module, which is not 100% compatible with POSIX Extended Regular Expression as specified in the RFC. For information about the Python re module, refer to http://docs.python.org/release/2.5.1/lib/module-re.html.
   • Replacement: This specifies the domain name for the next lookup. The default is a dot (.), which indicates that the regular expression in the REGEX field provides the replacement value. Alternatively, you can enter the replacement value in FQDN format.
   • Comment: Optionally, enter a descriptive comment for this record.
   • Disable: Clear the check box to enable the record. Select the check box to disable it.
3. Click Next to define extensible attributes. For information, see Using Extensible Attributes. This is not applicable when you configure a NAPTR record for a DTC server.
4. Save the configuration and click Restart if it appears at the top of the screen.

Managing LBDN Records

When your Grid has a DNS Traffic Control license, you can add LBDN (Load Balanced Domain Name) records to authoritative or delegated zones. You can add an LBDN even if the zone is DNSSEC signed but some restrictions apply.

To add an LBDN record when in the DNS records list view:

• On the Zones or Members/Servers tab, click the arrow next to the Add icon and select Record -> DTC LBDN. For more information, see Configuring DNS Traffic Control LBDNs.

You can also add an LBDN when in the Traffic Control tab. For more information, see the previously referenced section.

Viewing Resource Records

You can view the configured resource records by navigating to the Data Management tab -> DNS tab -> Zones tab -> zone -> Records tab. Grid Manager displays the following information for each resource record in the zone:

• Name: The name of the record, if applicable. For host records, this field displays the canonical name of the host. For PTR record, this displays the PTR record name without the zone name.
• Type: The resource record type.
• Data: Data that the record contains. For host records, this field displays the IP address of the host. For PTR records, this displays the
You can also show the following columns:

- **MSDelegationAddresses**: This column appears only if the primary server of the zone is a Microsoft server. It displays the IP addresses that are associated with an NS record.
- **TTL**: The TTL (time-to-live) value of the record.
- **Address**: The IPv4 or IPv6 address associated with the owner domain name in a reverse-mapping zone.
- **Shared**: Displays true for shared resource records. Otherwise, displays false.
- **SharedRecordGroup**: Displays the shared record group name of a shared record.
- **Disabled**: Indicates if the record is disabled.

You can do the following:

1. Modify some of the data in the table. Double click a row and either modify the data in the field or select an item from a drop-down list. Click **Save** to save the changes. Note that some fields are read-only.
2. Add new DNS records by clicking the arrow next to the Add icon and selecting **Host**, **Record**, **SharedRecord**, and then selecting the required record type. For more information, see Managing Resource Records.
3. View the DNS Traffic Control structure for an LBDN.
   - Select the LBDN record and click the Open Visualization icon. For more information, see Visualization for DNS Traffic Control Objects.
4. Create a DTC server based on an existing A, AAAA, or host record by selecting a record in the table and clicking **CreateDTCServer** in the Toolbar or in the record's Action menu. For more information, see Configuring DNS Traffic Control Servers.
5. Edit the properties of a resource record.
   - Select the resource record, and then click the **Edit** icon.
6. Delete a resource record.
   - Select the resource record, and then click the **Delete** icon.
7. Export the list of resource records to a .csv file.
   - Click the Export icon.
8. Print the list of resource records.
   - Click the Print icon.
9. Use filters and the **Goto** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Goto** field and select the object from the possible matches.
10. Create a quick filter to save frequently used filter criteria:
    1. In the filter section, click **Show Filter** and define filter criteria for the quick filter.
    2. Click **Save** and complete the configuration in the Save Quick Filter dialog box.

### Modifying, Disabling, and Deleting Host and Resource Records

You can modify, disable, or delete an existing host or DNS resource record. When physical repair or relocation of a network device occurs, you can disable a record instead of deleting it. When you disable a record, the NIOS appliance does not answer queries for it, nor does it include disabled records in zone transfers and zone imports. This avoids having to delete and then add the record again. When the changes to the physical device are complete, you can simply enable the host or resource record.

To modify or disable a host or resource record:

1. Use one of the following methods to retrieve the host or resource record:
   - Perform a global search.
   - Select it from a Smart Folder.
   - From the Data Management tab, select the DNS tab - > **Zones** tab - > **dns_view** - > zone - > host_record or resource_record.
2. Select the record you want to modify and click the Modify icon.
3. In the host or resource record editor, you can do the following:
   - In the General tab, you can change most of the information, except for the read-only fields, such as the **DNSView** and **HostName**
   - In the **TTL** tab, you can modify the TTL setting. The NIOS appliance also allows you to specify TTL settings for each record. If you do not specify a TTL for a record, the appliance applies the default TTL value of the zone to each record. For information, see About Time To Live Settings.
   - In the Extensible Attributes tab, you can modify the attributes. For information, see Using Extensible Attributes.
   - The Permissions tab displays if you logged in as a superuser. For information, see About Administrative Permissions.
4. Save the configuration and click **Restart** if it appears at the top of the screen.

When you delete host and resource records, Grid Manager moves them to the Recycle Bin. You can use the Recycle Bin to store deleted DNS configuration objects and selectively restore objects to the active configuration at a later time. You can also permanently remove the objects from
the Recycle Bin.

**Note:** You cannot delete automatically-generated records, such as NS records and SOA records.

To delete host and resource record:

1. Perform a global search to retrieve the record you want to delete.
   or
   From the Data Management tab, select the DNS tab, click the Zones tab -> dns_view -> zone -> host_record or resource_record.
2. Select the record and click the Delete icon.
3. In the Delete Confirmation dialog box, select Yes to delete or No to cancel.
4. Optionally, if the Enable PTR record removal for A/AAAA records option is selected and if you try to delete an A or AAAA record, the appliance displays the Delete Confirmation (A or AAAA Record) dialog box to confirm whether you want to remove the corresponding PTR record that was automatically generated while creating the A or AAAA record. In the Delete Confirmation dialog box, select the Remove associated PTR resource record(s) check box and click Yes to delete the associated PTR record or click No to cancel. For information about enabling this option, see Deleting PTR Records associated with A or AAAA Records.
   or
   You can also schedule the deletion for a later time. Click Schedule Deletion and in the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Deletions.

**About Shared Record Groups**

A shared record group is a set of resource records that you can add to multiple zones. You can create resource records in a group and share the group among multiple zones. The zones handle the shared resource records as any other resource record. You can include the following types of DNS resource records in a shared record group: A, SRV, MX, AAAA, CNAME, and TXT.

Using shared record groups simplifies and expedites the administration of resource records. When you create or update a shared record, the appliance automatically updates it in all associated zones. In addition, shared resource records reduce the object count in the NIOS database; instead of the creating the same record in multiple zones, you can use only one shared record. For example, for 10 zones and 500 records per zone, the object count decreases from 5278 objects to 781 objects.

*Figure 20.7* shows an example of how to create and use shared records.

In this example, there are two shared record groups. One group—group1—contains the A records ftp and printer1 and the MX record mx1, and the other group—group2—contains the A record web and the MX record mx2. The resource records in group1 are shared with the internal view zones sales.corpxyz.com and finance.corpxyz.com and the external view zone sales.corpxyz.com. The resource records in group2 are shared with the internal view zone marketing.corpxyz.com and the external view zones sales.corpxyz.com and marketing.corpxyz.com.

*Figure 20.7 Creating Shared Records*
The following are guidelines for using shared records:

- You can include multiple shared A, AAAA, CNAME, SRV, MX and TXT resource records in a group. You cannot include NS, DNAME, PTR, host and bulk host records.
- You can add shared records to authoritative zones only. You cannot add shared records to forward zones, stub zones, or reverse mapping zones.
- Zones that contain shared records can also contain regular DNS records (not shared).
- When you change or delete a shared resource record, it changes the canonical source of the shared record and impacts all the zones that contain the record.
- You cannot copy shared records from a zone.
- You do not need to restart the appliance when you create, delete, or modify shared records.

Configuring Shared Record Groups
Before you can create shared resource records, you must first create the group to which they belong. The shared record group serves as a container for the shared resource records. The following are the tasks to configure a shared record group:

1. Create a shared record group and associate it with the appropriate zones. See Creating a Shared Record Group.
2. Create shared A, CNAME, SRV, MX, AAAA, and TXT resource records, and add them into the shared record group. See Managing Shared Resource Records.

Creating a Shared Record Group
When you create a shared record group, the only requirement is that you give it a name. You can associate it with one or multiple zones when you first create the group or at a later time, by editing the shared record group. You can associate a shared record group with authoritative zones only. Associating the shared record group with a zone adds the shared records to the zone. The zone handles the shared records like any other resource records.

To create a shared record group:

1. From the Data Management tab, select the DNS tab -> Shared Record Groups tab, and then click the Add icon.
2. In the Shared Record Group wizard, specify the following:
   - **Name**: Enter the name of the shared record group. It can be up to 64 characters long and can contain any combination of printable characters. You can change the shared record group name even after you create the group. It does not impact the shared records in the group.
   - **Hostname Policy**: Click Override to supersede the hostname restriction policy set at the zone level or click Inherit to use the zone policy. This sets the hostname policy for the shared records in the group. See Specifying Hostname Policies.
   - **Comment**: Optionally, enter additional information about the shared record group.
3. Click Next to associate the shared record group with at least one zone.
4. Click the Add icon in the Associated Zones panel.
5. In the Zone Selector dialog box, select a zone by clicking the zone name. You can add multiple zones.
6. Click Next to define extensible attributes. For information, see Using Extensible Attributes.
7. Save the configuration.

Viewing Shared Record Groups
You can view the configured shared record groups by navigating to the Data Management tab -> DNS tab -> Shared Record Groups tab. Grid Manager displays the following information about each shared record group:

- **Name**: The shared record group name.
- **Comment**: Comments that were entered for the shared record group.
- **Site**: Values that were entered for this pre-defined attribute.

You can do the following:

- List the shared resource records and associated zones in a shared record group.
- Click a shared record group name.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
- Edit the properties of a shared record group.
  - Click the check box beside a shared record group, and then click the Edit icon.
- Delete a shared record group.
  - Click the check box beside a shared record group, and then click the Delete icon. Note that you must remove the zone associations in a shared record group before you delete it.
- Export the list of shared record groups to a .csv file.
Click the Export icon.
Print the list of shared record groups.
Click the Print icon.

Modifying a Shared Record Group

When you edit a shared record group, you can do the following:

1. Perform a global search to retrieve the shared record group you want to modify.
   or
   From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group check box, and then click the Edit icon.
2. The Shared Record Group editor contains the following tabs from which you can modify information:
   • General: You can change any of the information you entered when you created it, including its name. Changing the shared record group name does not impact the shared resource records in it.
   • Extensible Attributes: You can modify the attributes. For information, see Using Extensible Attributes.
   • Permissions: This tab is displayed if you logged in as a superuser. For information, see About Administrative Permissions.
3. Save the configuration and click Restart if it appears at the top of the screen.

Deleting Shared Record Groups

Before you delete a shared record group, you must remove the zone associations in the group; otherwise, an error message appears when you delete. For information, see Deleting Associated Zones.
To delete a shared record group:

1. Perform a global search to retrieve the shared record group you want to modify.
   or
   From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group check box, and then click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes.

Grid Manager moves the shared record group to the Recycle Bin, if enabled. Use the Recycle Bin feature to recover a deleted shared record group and retrieve the deleted zones. For information, see Using the Recycle Bin.

Managing Shared Resource Records

You can create shared A, AAAA, CNAME, MX, SRV and TXT records. These resource records are similar to the non-shared resource records. The DNS server uses them to respond to queries in the same way as any other resource record. A shared resource record can belong to only one shared record group. This section describes how to add shared resource records to a group and how to modify and delete them. It includes the following sections:

- Creating Shared Records
- Viewing Shared Records
- Modifying Shared Records
- Deleting Shared Records

NIOS allows superusers to add shared A and AAAA records with a blank name. Limited-access users must have read/write permission to Adding a blank A/AAAA record to add shared A and AAAA records with a blank name. You can assign global permission for specific admin groups and roles to allow limited-access users to add shared A and AAAA records with a blank name. For more information, see Administrative Permissions 1 or Adding Blank A or AAAA Records.

Creating Shared Records

After you create a shared record group, you can create its resource records. To create a shared A, AAAA, CNAME, MX, SRV or TXT record and add it to a group:

1. From the Data Management tab, select the DNS tab. Expand the Toolbar and click Add -> Shared Record.
   or
   From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group. Expand the Shared Records tab and click the Add icon.
2. Select one of the following:
   • Shared A Record
   • Shared AAAA Record
   • Shared CNAME Record
   • Shared MX Record
   • Shared SRV Record
   • Shared TXT Record
3. Enter information in the Shared Record wizard. See the online Help or the following for information about each resource record:
   • For information about A records, see Managing A Records.
   • For information about AAAA records, see Managing AAAA Records.
   • For information about CNAME records, see Managing CNAME Records.
For information about MX records, see Managing MX Records.
For information about SRV records, see Managing SRV Records.
For information about TXT records, see Managing TXT Records.

4. Save the configuration, or click Next to define extensible attributes for the shared record. For information, see Using Extensible Attributes.

5. Click Restart if it appears at the top of the screen.

Viewing Shared Records

You can view the shared records in a group and in a zone. To edit the shared record properties, click the shared record name and select the Edit icon.

To view the shared records in a group:

- From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group -> Shared Records tab.

To view the shared records in a zone:

- From the Data Management tab, select the DNS tab -> Zones tab and select a zone. Grid Manager lists the following information about each shared record by default:
  - **Name**: The shared record name.
  - **Type**: Indicates the type of resource record, such as A, AAAA, CNAME, MX, SRV or TXT records. Shared records are identified as *(Shared)*.
  - **Data**: The data the shared resource record provides.
  - **Comment**: Comments that were entered in the resource record.
  - **Site**: Displays values that were entered for this pre-defined attribute.

You can display the following additional columns:

- **TTL**: The TTL value of the shared resource record.
- **Disabled**: Indicates whether the record is disabled.

You can do the following:

- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
- Edit the properties of a shared resource record.
  - Select the shared resource record, and then click the Edit icon.
- Delete a shared resource record.
  - Select the shared resource record, and then click the Delete icon.
- Export the list of shared resource records to a .csv file.
  - Click the Export icon.
- Print the list of shared resource records.
  - Click the Print icon.

Modifying Shared Records

You can modify, disable, or delete any shared record. When physical repair or relocation of a network device occurs, you can disable a record instead of deleting it. This alleviates having to delete, and then add the shared record again. When the changes to the physical device are complete, you can simply enable the shared record.

To modify or disable a shared record:

1. Perform a global search to retrieve the host or resource record you want to modify.
   or
   From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group -> Shared Records tab.
2. Select the shared record you want to modify and click the Edit icon.
3. The Shared Records editor contains the following tabs from which you can modify information:
   - **General**: You can change most of the information, except for the read-only fields, such as the Host Name Policy. You can also select the Disable check box to disable the record.
   - **TTL**: You can modify the TTL setting. For information, see About Time To Live Settings.
   - **Extensible Attributes**: You can modify the attributes. For information, see Using Extensible Attributes.
   - **Permissions**: This tab displays if you logged in as a superuser. For information, see About Administrative Permissions.
4. Save the configuration and click Restart if it appears at the top of the screen.

Deleting Shared Records

To delete shared resource records:
1. Perform a global search to retrieve the record you want to delete.
   or
   From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group -> Shared Records tab.
2. Select the shared record you want to delete and click the Delete icon.
3. When the confirmation dialog box displays, select Yes.

Grid Manager moves the shared records to the Recycle Bin, from which you can restore or permanently delete the records.

Managing Associated Zones

Typically, you associate a zone with a shared record group when you create the group. You can also add an associated zone to a shared record group after you create the group.

Creating Associated Zones

To associate a zone with a share record group:

1. From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group -> Associated Zones tab, and then click the Add icon.
2. In the Zone Selector dialog box, select a zone by clicking the zone name.

The appliance adds the zone to the Associated Zones tab.

Viewing Associated Zones

To view the associated zones in a shared record group:

- From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group -> Associated Zones tab.

Grid Manager lists the following information about each associated zone by default:

- **Zone**: The zone associated with the shared record group.
- **DNS View**: The DNS view to which the zones belong.
- **Network View**: The network view associated with the DNS view.
- **Comment**: Comments that were entered for the shared record group. You can do the following:
  - Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
  - Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
  - Associate another zone with the shared record group.
    - Click the Add icon and select a zone.
  - Select an associated zone.
  - Select the zone, and then click the Delete icon.
  - Export the list of associated zones to a .csv file.
    - Click the Export icon.
    - Print the list of shared associated zones.
      - Click the Print icon.

Deleting Associated Zones

To delete an associated zone:

1. From the Data Management tab, select the DNS tab -> Shared Record Groups tab -> shared_record_group -> Associated Zones tab.
2. Select the associated zone and click the Delete icon.
3. When the confirmation dialog box displays, select Yes.

Grid Manager removes the zone from the shared record group.

Configuration Example: Configuring Shared Records

The following example shows you how to configure shared records. In this example, you do the following:

- Create a shared record group: **group1**.
- Associate it with three zones: **eng.com**, **sales.com**, and **marketing.com**.
- Create an A record **www** and an MX record **mx1**.

1. Create a shared record group called **group1** and associate it with **eng.com**, **sales.com**, and **marketing.com**.
1. From the Data Management tab, select the DNS tab -> Shared Record Groups tab, and then click the Add icon.
   a. In the first step of the Shared Record Group wizard, specify the following Name: Enter group1.
   b. Click Next.
   c. Click the Add icon in the Associated Zones panel.
   d. Select eng.com from the list of zones and click the select icon. Do the same for the sales.com, and marketing.com zones.
   e. Save the configuration and click Restart if it appears at the top of the screen.

2. Add an A record www to group1.
   a. Expand the Toolbar and click Add -> Shared Record > Shared A Record.
   b. In the Shared A Record wizard, specify the following:
      Name: Enter www.
      Shared Record Group: Select group1 from the drop-down list.
      IP Address: Enter the IP address 10.9.1.1.
   c. Save the configuration and click Restart if it appears at the top of the screen.

3. Add an MX record mx1 into group1.
   a. Expand the Toolbar and click Add -> Shared Record > Shared MX Record.
   b. In the Shared MX Record wizard, specify the following:
      Mail Destination: Enter mx1.
      Shared Record Group: Select group1 from the drop-down list.
      Comment: Enter mail exchanger record for shared record group1.
   c. Save the configuration and click Restart if it appears at the top of the screen.

Chapter 21 Configuring DDNS Updates

DDNS (Dynamic DNS) is a method to update DNS data (A, TXT, and PTR records) from sources such as DHCP servers and other systems that support DDNS updates, such as Microsoft Windows servers 2000, 2003, 2008, 2008 R2, 2012, 2012 R2, and 2016. This chapter provides conceptual information about DDNS and explains how to configure NIOS appliances running DHCP, DHCPv6 and DNS to support DDNS updates. It contains the following main sections:

- Configuring DHCP for DDNS
  - Configuring DHCP Features
    - Resending DDNS Updates
    - Generating Host Names for DDNS Updates
    - Configuring DDNS Features
    - Replacing Host Names for DDNS Updates
  - About the Client FQDN Option
    - Enabling FQDN Option Support
    - Sending Updates for DHCP Clients Using the FQDN Option
  - Configuring DDNS Update Verification
  - Configuring DNS Servers for DDNS
    - Enabling DNS Servers to Accept DDNS Updates
    - Forwarding Updates
  - Supporting Active Directory
    - Sending DDNS Updates to a DNS Server
  - About GSS-TSIG
    - Sending Secure DDNS Updates to a DNS Server in the Same Domain
    - Configuring DHCP to Send GSS-TSIG Updates in the Same Domain
    - Sending Secure DDNS Updates to a DNS Server in Another Domain
    - Configuring DHCP to Send GSS-TSIG Updates to Another Domain
    - Sending GSS-TSIG Updates to a DNS Server in Another Forest
  - Configuring GSS-TSIG keys
    - Limitations when Using Multiple GSS-TSIG keys
    - Scheduled Upgrade
    - Admin Permissions for Configuring GSS-TSIG keys
    - Enabling GSS-TSIG Authentication for DHCP
    - Deleting GSS-TSIG keys associated with DHCP Objects
    - Enabling GSS-TSIG Authentication for DNS
    - Deleting GSS-TSIG keys associated with the DNS Objects
    - Logging Messages
    - Managing GSS-TSIG keys
    - Selecting Keys in the GSS-TSIG Key Selector
  - Accepting DDNS Updates from DHCP Clients
    - Accepting GSS-TSIG-Authenticated Updates
  - Configuring DNS to Receive GSS-TSIG Updates
  - Secure Dynamic Updates
    - Restricting Updates to Static Records
Restricting Updates to Protected Records
Restricting Updates Based on GSS-TSIG Principal Authentication
Restricting Updates Based on FQDN Patterns

Understanding DDNS Updates from DHCP

DHCP supports several DNS-related options (such as options 12, 15, and 81 for IPv4, and options 23, 24, and 39 for IPv6). With DDNS (Dynamic DNS) updates, a DHCP server or client can use the information in these options to inform a DNS server of dynamic domain name-to-IP address assignments.

**Note:** DDNS updates is not supported by IPv6-only appliances.

To set up one or more NIOS appliances for DDNS updates originating from DHCP, you must configure at least one DHCP server and one DNS server. These servers might be on the same appliance or on separate appliances. Three possible arrangements for a DHCP server to update a DNS server are shown in Figure 21.1.
Figure 21.1 Relationship of DHCP and DNS Servers for DDNS Updates

Figure 21.2 When an IPv4 DHCP client requests an IP address, the client sends its host name (DHCP option 12). The client also includes its MAC address in the ethernet frame header.

1. When an IPv4 DHCP client requests an IP address, the client sends its host name (DHCP option 12). The client also includes its MAC address in the ethernet frame header.

2. When the DHCP server responds with an IP address, it usually provides a domain name (DHCP option 15). The combined host name (from the client) and domain name (from the server) form an FQDN (fully qualified domain name), which the NIOS appliance associates
with the IP address in the DHCP lease.

b. The DHCP server sends the A, TXT, and PTR records of the DHCP client to the primary DNS server to update its resource records with the dynamically associated FQDN + IP address.

3. The primary DNS server notifies its secondary servers of a change. The secondary servers confirm the need for a zone transfer, and the primary server sends the updated zone data to the secondary server, completing the update.

**Note:** For information about zone transfers, see *Enabling Zone Transfers*.

---

**Figure 21.2 DDNS Update from a DHCP Server**

To enable a DHCP server to send DDNS updates to a DNS server, you must configure both servers to support the updates. First, configure the DHCP server to do the following:

- Provide what is needed to create an FQDN: add a server-generated host name to a server-provided domain name, add a server-provided domain name to a client-supplied host name, or permit the client to provide its own FQDN
- Send updates to a DNS server

Then, configure the following on the DNS server:

- Accept updates from the DHCP server, a secondary DNS server, or a DHCP client
- If the DHCP server sends updates to a secondary DNS server, configure the secondary server to forward updates to the primary DNS server

When setting up DDNS, you can determine the amount of information that DHCP clients provide to a DHCP server — and vice versa — and where the DDNS updates originate. A summary of these options for IPv4 is shown in bookmark1920. It is similar for IPv6, except that the DHCP client and server exchange Request and Reply messages, AAAA records are updated instead of A records, and the FQDN option is option 39.

**Figure 21.3 DHCP Clients and Server Providing DNS Information and Updates**
You can configure the DHCP and DNS settings for DDNS at the Grid level, member level, and network and zone level. By applying the inheritance model in the NIOS appliance, settings made at the Grid level apply to all members in the Grid. Settings you make at the member level apply to all networks and zones configured on that member. Settings made at the network and zone level apply specifically to just that network and zone. When configuring independent appliances (that is, appliances that are not in a Grid), do not use the member-level settings. Instead, configure DDNS updates at the Grid level to apply to all zones and, if necessary, override the Grid-level settings on a per zone basis.

Configuring DHCP for DDNS

Before a DHCP server can update DNS, the DHCP server needs to have an FQDN-to-IP address mapping. When a DHCP IPv4 client requests an IP address, it typically includes its host name in option 12 of the DHCPDISCOVER packet, and an IPv6 client includes its hostname in the Request packet. You can configure the NIOS appliance to include a domain name in option 15 of the IPv4 DHCPOFFER packet or in the IPv6 Reply packet. You specify this domain name in the IPv4 DHCP Options -> Basic and IPv6 DHCP Options -> Basic tabs of the Grid DHCP Properties editor, Member DHCP Configuration editor, and the Network editor. For IPv4 clients you can also specify a domain name in the DHCP Range and Fixed Address editors.

Then, you can enable the DHCP server to send DDNS updates for IPv4 and IPv6 clients, as described in 4817228 4817228. After you enable the DHCP server to send DDNS updates, you can do the following:

- Configure the DHCP server to send DDNS updates to DNS servers in the Grid. For information, see 4817228 4817228.
- Configure the DHCP server to send DDNS updates to external DNS servers. For information, see Configuring DDNS Features.
- Configure certain DDNS features. For information, see Configuring DDNS Features.
- Enable support for the FQDN option for IPv4 and IPv6 clients, and configure how the DHCP server updates DNS. For information, see En
Note: Whether you deploy NIOS appliance in a Grid or independently, they send updates to UDP port 53. Grid members do not send updates through a VPN tunnel; however, Grid members do authenticate updates between each other using TSIG (transaction signatures) based on an internal TSIG key.

Enabling DDNS for IPv4 and IPv6 DHCP Clients

You can enable the DHCP server to send DDNS updates for IPv4 clients at the Grid, member, shared network, network, address range, DHCP template, fixed address, and roaming host levels, and for IPv6 clients at the Grid, member, network, shared network, network template and roaming host levels.

You can specify a different domain name that the appliance uses specifically for DDNS updates. The appliance combines the hostname from the client and the domain name you specify to create the FQDN that it uses to update DNS. For IPv4 clients, you can specify the DDNS domain name at the network, network template, range, and range template levels. For IPv6 clients, you can specify the DDNS domain name at the Grid, member, network, shared network, and network template levels. You can also use the name of a roaming host record as the name of the client for DDNS updates, as described in Setting Properties for Roaming Hosts.

To enable DDNS and specify a DDNS domain name:

1. Grid: From the Data Management tab, select the DHCP tab, expand the Toolbar and click Grid DHCP Properties. Member: From the Data Management tab, select the DHCP tab and click the Members tab -> Members -> member check box -> Edit icon. Network: From the Data Management tab, select the DHCP tab and click the Networks tab -> Networks -> network check box -> Edit icon. Network Container: From the Data Management tab, select the IPAM tab -> network_container check box, and then click the Edit icon. Network Template: From the Data Management tab, select the DHCP tab and click the Templates tab -> DHCP_template check box -> Edit icon. Roaming Host: From the Data Management tab, select the DHCP tab and click the Networks tab -> Roaming Hosts -> roaming_host - > Edit icon. IPv4 Address Range: From the Data Management tab, select the DHCP tab and click the Networks tab -> Networks -> network -> ip_a rks -> network -> addr_range check box -> Edit icon. IPv4 Fixed Address: From the Data Management tab, select the DHCP tab and click the Networks tab -> Networks -> network -> ip_a ddr check box -> Edit icon. IPv4 Address Range/Fixed Address Template: From the Data Management tab, select the DHCP tab and click the Templates tab -> DHCP_template check box -> Edit icon.

To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the IPv4 DDNS -> Basic tab or the IPv6 DDNS -> Basic tab, complete the following:
   - Enable DDNS Updates: Select this check box to enable DDNS updates. When setting properties for DHCP objects other than the Grid, you must click Override and select Enable DDNS updates for the DDNS settings to take effect.

Note: When setting properties for DHCP objects other than the Grid, you must click Override and select Enable DDNS updates for the DDNS settings to take effect. When turning on DDNS updates, first verify if option 81 has been enabled and whether DNS is being updated. If DNS is being updated, even if the DNS zone targets are not in the Grid, select Option 81 support and the correct suboption. For more information, see Enabling FQDN Option Support.

When the Enable DDNS Updates check box is not selected, the default behaviour is to allow the client to update DNS. When the Enable DDNS Updates check box is selected, the default behaviour is to prevent DDNS updates from the client.

Note: In a dual mode Grid, if IPv6 DDNS updates is enabled at the Grid level, then when you join an IPv6 Grid member to the Grid, IPv6 DDNS updates is automatically disabled for the Grid member.

- DDNS domainname: Specify the domain name of the network that the appliance uses to update DNS. For IPv4 clients, you can specify this at the network, network template, range, and range template levels. For IPv6 clients, you can specify this at the Grid, member, network, shared network, and network template levels.

- DDNSUpdateTTL: You can set the TTL used for A or AAAA and PTR records updated by the DHCP server. The default is shown as zero. If you do not enter a value here, the appliance by default sets the TTL to half of the DHCP lease time with a maximum of 3600 seconds. For example, a lease time of 1800 seconds results in a TTL of 900 seconds, and a lease time of 86400 seconds results in a TTL of 3600 seconds. For information about how to set the lease time, see Defining Lease Times.

- DDNSUpdateMethod: Select the method used by the DHCP server to send DDNS updates. You can select either Interim or Standard from the drop-down list. The default is Interim. When you select Interim, TXT record will be created for DDNS updates and when you select Standard, DHCPD record will be created for DDNS updates. But in the IPv4DDNS -> Advanced tab, if you have selected NoTXTRecord mode for the DHCP server to use when handling DNS updates, then TXT record or DHCPD record is not created for DDNS updates.
If you change the DDNS update method from Interim to Standard or vice versa, then the DHCP server changes the DHCID type used from TXT record to DHCID record or vice versa as the leases are renewed.

This is supported for clients that acquire both IPv4 and IPv6 leases. Infoblox recommends you to configure different DDNS update method for IPv4 leases and IPv6 leases, Interim for IPv4 lease and Standard for IPv6 lease.

- **UpdateDNSonDHCPLeaseRenewal**: Select this check box to enable the appliance to update DNS when a DHCP lease is renewed.

3. Save the configuration and click Restart if it appears at the top of the screen.

### Sending Updates to DNS Servers

The DHCP server can send DDNS updates to DNS servers in the same Grid and to external DNS servers. When you enable the appliance to send updates to Grid members, you must specify the DNS view to be updated. If a network view has multiple DNS views, you can select only one DNS view for DDNS updates. For information about DNS views, see Using Infoblox DNS Views.

When you enable DDNS updates for a Grid, member, shared network, network, address range, DHCP template, fixed address, or roaming host, the DHCP server sends updates to authoritative zones using the domain name (as DHCP option 15) you define in the DHCP properties. You can also define forward-mapping zones that receive DDNS updates for DHCP clients that use option 81 to define the domain name. For information, see About the Client FQDN Option. To allow DDNS updates for clients using option 81, you must first enable the support for option 81. For information, see Configuring DDNS Features.

For DNS zones that have multiple primary servers, you can define a primary name server to be used as the default primary server when performing DDNS updates from the appliance. Note that you cannot configure an external primary as the default primary. For more information, see 4817228 4817228.

### Sending Updates to DNS Servers in the Grid

You must specify the DNS view to be updated for each network view.

To configure the DHCP server to send updates to DNS servers in the same Grid:

1. If there are multiple network views in the Grid, select a network view.
2. From the DataManagement tab, select the DHCP tab, and then click ConfigureDDNS from the Toolbar.
3. In the DDNS Properties editor, complete the following:
   - **DNS View**: If a network view has more than one DNS view, this field lists the associated DNS views. From the drop-down list, select the DNS view to which the DHCP server sends DDNS updates. Otherwise, the appliance uses the default DNS view.

4. Save the configuration and click Restart if it appears at the top of the screen.

The appliance sends DDNS updates to the appropriate zones in the selected DNS view. Note that you cannot delete a DNS view that has been selected for DDNS updates. By default, the DHCP server sends DDNS updates to zones using the domain name that you define for DHCP objects, such as networks and DHCP ranges.

### Sending Updates for Zones on an External Name Server

The DHCP server can send dynamic updates to an external name server that you specify. For each network view, you can specify the zone to be updated and the IP address of the primary name server for that zone. You can add information for a forward and reverse zone. The DHCP server updates the A record in the forward zone and the PTR record in the reverse zone.

You can also use TSIG (transaction signatures) or GSS-TSIG to secure communications between the servers. TSIG uses the MD5 (Message Digest 5) algorithm and a shared secret key to create an HMAC (hashed message authentication code)—sometimes called a digital fingerprint—of each update. Both the DHCP server sending the update and the DNS server receiving it must share the same secret key. Also, it is important that the time stamps on the TSIG-authenticated updates and update responses be synchronized, or the participants reject them.

Therefore, use an NTP server to set the time on all systems involved in TSIG authentication operations. Note that only a superuser can configure DDNS. To configure DDNS, a limited-access admin must contact a superuser.

To send updates to a DNS server that is external to your Grid:

1. If there are multiple network views in the Grid, select a network view.
2. From the DataManagement tab, select the DHCP tab, expand the Toolbar and click ConfigureDDNS.
3. In the DDNSUpdatestoExternalZones section of the DDNSProperties editor, click the Add icon. Complete the following fields in the Add External DDNS Zone panel, and then click Add:
   - **ZoneName**: Enter the FQDN of a valid forward-mapping or reverse-mapping zone to which the DHCP server sends the updates. Do not enter the zone name in CIDR format. To specify a zone name in IDN, manually convert IDN to punycode and use the punycode representation.
   - **DNSServerAddress**: Enter the IP address of the primary name server for that zone.
   - **Security**: Select one of the following security methods:
     - **None**: Select this to use unsecured DDNS updates. This is the default.
     - **TSIG**: Select this to use the standards-based TSIG key that uses the one-way hash function MD5 to secure transfers between name servers. You can either specify an existing key or generate a new key.
To specify an existing key, complete the following:

- **KeyName**: Enter the TSIG key name. The key name entered here must match the TSIG key name on the external name server.
- **KeyAlgorithm**: Select either HMAC-MD5 or HMAC-SHA256.
- **KeyData**: To use an existing TSIG key, type or paste the key in the **KeyData** field. Alternatively, you can select the key algorithm, select the key length from the **GenerateKeyData** drop down list, and then click **GenerateKeyData** to create a new key.
  - **GSS-TSIG**: For information about using GSS-TSIG, see About GSS-TSIG.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Defining the Default Primary for DDNS Updates to Zones with Multiple Primaries

If you have configured multiple primary servers for an authoritative zone, you can define the default primary that the appliance uses to perform DDNS updates for the zone. Note that you can configure a Grid primary, but not an external primary, as the default primary. If you do not configure a default primary, the Grid Master becomes the default primary for the zones that it serves. Otherwise, the appliance selects a primary server that serves the zone as the default primary. For external zones that have multiple primaries, the first external primary server becomes the default primary.

Configuring a default primary for DDNS updates is useful when you have DHCP members that span across different locations. Performing DDNS updates becomes more efficient when you configure a default primary that is close in proximity to the DHCP member. For example, zone corpxyz.com has two primaries (usa.corpxyz.com and japan.corpxyz.com) serving two locations (USA and Japan). Service performance is faster when you select usa.corpxyz.com as the default primary for DDNS updates in the USA region and japan.corpxyz.com as the default primary for the Japan region.

When you configure a preferred or default primary server for DDNS updates to a zone that has multiple primaries, ensure that the following are in place:

- The zone that you select contains multiple primary servers.
- The primary server has DNS service enabled and is authoritative for the zone.
- The appliance has DHCP service enabled.

**Note**: You can define the default primary for the Grid and override the setting at the member level, and you must restart service for the configuration to take effect. Primary selection is performed at service restart, not at runtime.

To define the default primary:

1. **Grid**: From the **Data Management** tab, select the **DHCP** tab, expand the Toolbar and click **Configure DDNS**. In the DDNS Properties editor, scroll down to the **Master Preferences for DDNS Updates to Multi-master DNS Zones** section.
2. **Member**: From the **Data Management** tab, select the **DHCP** tab and click the **Members** tab -> member check box -> Edit icon. In the **Member DHCP Properties** editor, select the **DNS** tab.
3. In the **Master Preferences for DDNS Updates to Multi-master DNS Zones** section, click the **Add** icon and select one of the following from the list:
   - **Grid Zone**: In the Add Grid Zone panel, complete the following:
     - **Zone**: Click **Select Zone** to select the zone that has multiple primaries. Note that when configuring for the Grid, only zones that belong to the selected DNS view are displayed in the Zone Selector dialog box. For a Grid member however, if it is associated with a network view or if you have defined a DNS view for DDNS updates for that network view, only zones that belong to the DNS view configured for the associated network view are displayed.
     - **DNS View**: Displays the DNS view to which this zone belongs.
     - **DNS Primary**: From the drop-down list, select the primary name server you want the appliance to use when performing DDNS updates. Note that the list displays only primary servers that are defined for the selected zone.
   - **Default Primary**: In the Add Default Primary panel, complete the following:
     - **DNS Primary**: Click **Select** to select a primary name server from the **Member Selector** dialog. When you select a default primary, the appliance uses this name server for DDNS updates to all zones.
4. Click **Add** to add the zone and primary name server to the table, which displays the following information:
   - **DNS View**: The DNS view to which the zone belongs.
   - **Zone**: The selected zone that has multiple primaries.
   - **DNS Primary**: The primary server to be used when performing DDNS updates from a NIOS DHCP server to the selected zone.

**Note**: All zones added to the table belong to the same DNS view.
Concatenated with the following rules defined at the Grid level: This section appears only in the Member DHCP Properties editor. This table displays rules that are defined for zones with multiple primaries at the Grid level. Rules configured at the member level automatically override those configured for the Grid. Note that all rules configured for both the Grid and the member apply.

Configuring DDNS Features

You can enable the DHCP server to support certain DDNS features for IPv4 and IPv6 clients. These features affect the behavior of the DHCP server and how it handles DDNS updates. The following sections describe the different features you can set.

Resending DDNS Updates

You can enable the DHCP server to make repeated attempts to send DDNS updates to a DNS server. The DHCP server asynchronously updates DNS for a particular lease and sends the DHCP ACK to the client requesting the lease. If the update fails, the DHCP server still provides the lease and sends the DHCP ACK to the client. The DHCP server then continues to send the updates until it is successful or the lease of the client expires. You can change the default retry interval, which is five minutes. You can enable this feature for the Grid and for individual Grid members.

Generating Host Names for DDNS Updates

Some IPv4 and IPv6 clients do not send a host name with their DHCP requests. When the DHCP server receives such a request, its default behavior is to provide a lease but not update DNS. You can configure the DHCP server to generate a host name and update DNS with this host name when it receives a DHCP request that does not include a host name. It generates a name in the following format: dhcp-ip_address, where ip_address is the IP address of the lease. For example, if this feature is enabled and the DHCP server receives a DHCP REQUEST from an IPv4 DHCP client with IP address 10.1.1.1 and no host name, the DHCP server generates the name dhcp-10-1-1-1 and appends the domain name, if specified, for the DDNS update. Likewise, if an IPv6 client with IP address 2001:db8:a23:0:0:0:0:d sends a request, the DHCP server generates the name dhcp-2001-db8-a23-0-0-0-0-d and appends the domain name, if specified, for the DDNS update.

Updating DNS for IPv4 Clients with Fixed Addresses

By default, the DHCP server does not update DNS when it allocates an IPv4 or IPv6 fixed address to a client. You can configure the DHCP server to update the A and PTR record of IPv4 clients with a fixed address. When you enable this feature and the DHCP server adds A and PTR records for a fixed address, the DHCP server never discards the records. When the lease of the client terminates, you must delete the records manually. Note that the DHCP server does not send DDNS updates for IPv4 fixed addresses and hosts.

You can define fixed address settings for the Grid, Grid members, IPv4 networks, and IPv4 shared networks.

Configuring DDNS Features

You can configure DDNS features for a Grid, its member, IPv4 and IPv6 networks and shared networks, and IPv4 DHCP address ranges. You cannot set DDNS features for IPv6 DHCP ranges. To configure DDNS features:

1. **Grid:** From the Data Management tab, select the DHCP tab, expand the Toolbar and click Grid DHCP Properties. **Member:** From the Data Management tab, select the DHCP tab and click the Members tab -> member check box -> Edit icon.
   
   **Network:** From the Data Management tab, select the DHCP tab and click the Networks tab -> Networks -> network check box -> Edit icon.
   
   **Shared Network:** From the Data Management tab, select the DHCP tab and click the Networks tab -> Shared Networks -> shared_network check box -> Edit icon.
   
   **DHCP Range:** From the Data Management tab, select the DHCP tab and click the Networks tab -> Networks -> addr_range check box -> Edit icon.
   
   To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the DDNS -> Advanced tab for the Grid and member, or the DDNS -> Basic tab for the network, do the following:
   - **Update Retry:** You can set this for a Grid and its members only.
     - **Retry Updates When Server Becomes Available:** Select this check box.
     - **Retry Interval (Minutes):** You can optionally set the retry interval. The default is five minutes.
   - **Generate Hostname**
     - **Generate Hostname if not Sent by Client:** Select this check box to enable the DHCP server to generate a hostname and update DNS with this hostname, when the DHCP request of a client does not include a hostname.
   - **Fixed Address Updates:** You can set this for IPv4 fixed addresses only. This option is available in the IPv4 DDNS Advanced tab of the Grid DHCP Properties and Member DHCP Properties editors, and in the IPv4 DDNS Basic tab of the IPv4 DHCP Network and Shared Network editors.
     - **Update Fixed Addresses:** Select this check box to allow the DHCP server to send updates to DNS for IPv4 fixed addresses.

3. Save the configuration and click Restart if it appears at the top of the screen.

When a lease expires, the DHCP server removes the A, AAAA, and PTR records that it updated. It does not remove any records that the client
Replacing Host Names for DDNS Updates

In situations where you need to restrict the use of specific characters in a host name for DDNS updates, you can configure a hostname rewrite policy. Such policy accepts certain characters and replaces others in host names specified in IPv4 DHCP requests. When you create a hostname rewrite policy, you enter a list of valid characters that the appliance accepts in the host name. You also specify a character that the appliance uses to replace invalid characters. You can create multiple hostname rewrite policies on the appliance, but you can only enable one policy at any given time. The appliance provides a default policy that includes `a-z0-9_` as valid characters and dash (`-`) as the replacement character. You cannot modify or delete the default policy.

When you enable a hostname rewrite policy, the appliance replaces host names with the newly translated host name when it issues DHCP leases and sends DDNS updates for IPv4 DHCP clients. For information about how to add and enable a hostname rewrite policy, see Adding andEnabling a Hostname Rewrite Policy.

Before you enable a hostname rewrite policy, consider the following:

- You must enable DDNS updates before the hostname rewrite policy can take effect.
- You can use a hostname rewrite policy only if MS code pages are disabled.
- The policy supports only IPv4 DHCP clients.
- If DHCP option 81 support is enabled and updating DDNS is in the request, the appliance sends updates for A records directly to the DNS server and DHCP only updates the PTR record. When this happens, there can be a mismatch in the host name between the A and PTR records.
- Changes made to a hostname rewrite policy apply only to subsequent DDNS updates.

When an IPv4 DHCP client requests an IP address, it includes its host name in DHCP option 12. If you enable a hostname rewrite policy, the appliance uses the newly translated host name when it issues a lease to the client.

The client can also include a FQDN in option 81, in which it instructs the server whether to perform DDNS updates. If the client sends a FQDN in option 81, the appliance replaces the entire FQDN based on the policy. For example, if the FQDN in option 81 is dev.bldg12.corpxyz.com, the appliance replaces invalid characters in the entire FQDN even though the host name can be dev or dev.bldg12.corpxyz.com. For example, if your hostname rewrite policy specifies valid characters as `a-z` and the replacement character is `--`, the newly translated FQDN is dev.bldg--.corp--.com. For information about client FQDN in option 81, see About the Client FQDN Option.

Note that when multiple IPv4 DHCP clients specify host names that map to the same translated host name, the appliance allocates leases to all clients, but it only sends DDNS updates to the first client request. When it tries to update DNS for subsequent clients, the updates fail.

You can add and enable a hostname rewrite policy for the entire Grid. You can also override the policy at a member level, as described in Overriding a Grid Hostname Rewrite Policy.

Adding and Enabling a Hostname Rewrite Policy

To add and enable a hostname rewrite policy, complete the following:

1. From the Data Management tab, select the DHCP tab, expand the Toolbar and click Grid DHCP Properties.
2. In the Grid DHCP Properties editor, click Toggle Advanced Mode.
3. In the IPv4 DDNS -> Advanced tab, click the Add icon in the Hostname Rewrite Policy section:
   - **Policy Name**: Enter the policy name. Each policy name must be unique.
   - **Valid Characters**: Enter a list of valid characters you want to keep in the host name. Ensure that you consider the following rules:
     - You can include only printable ASCII characters and space.
     - The appliance includes period (`.`) as a valid character by default. You do not need to specify it.
     - You can also use shortcuts for a series or range of characters. For example, when you enter `a-d`, the appliance includes the following: A, B, C, D, a, b, c, and d. When you enter 0-5, the appliance includes the following: 0, 1, 2, 3, 4, and 5. In a character range, ensure that the start character is less than the end character.
     - If you want to use dash (`-`) as a character, ensure that you put it in front of the valid character pattern. Otherwise, the appliance treats the string as a range of characters.
     - You can build a POSIX regular expression based on the string you enter here, but you cannot enter an empty string.
     - You cannot use the meta character (`^`) as a start or end character in a range. For example, `a-^` is invalid. You also cannot use duplicate characters as character sets. For example, `aa` is invalid.
   - **Replace Invalid Characters with**: Enter a character the appliance uses to replace invalid characters. Only enter one printable ASCII character. You cannot enter multiple characters or use space as the replacement character.

To test the hostname policy before adding it to the system, enter a sample hostname in the Sample Host Name field, and then click Test. The appliance displays the translated hostname. You can change the policy and test it again until you get the desired result. Click the Add icon to add the new hostname rewrite policy to the table. The appliance comes with a default policy that includes `a-z0-9_` as valid characters and dash (`-`) as the replacement character. Grid Manager displays the following for each policy:
   - **Policy Name**: The name of the hostname rewrite policy.
   - **Valid Characters**: Valid characters for the host name.
   - **ReplaceInvalidCharacterswith**: The character used to replace invalid characters in the host name.

You can also select a hostname policy and click the Edit icon to modify it, or click the Delete icon to delete it. You cannot modify or delete the default policy. For information about how to modify a policy, see Modifying a Hostname Rewrite Policy.

4. Complete the following to enable the hostname rewrite policy:
Enable hostname rewrite policy: Select this check box to use a hostname rewrite policy for DHCP leases and DDNS updates for IPv4 DHCP clients. From the drop-down list, select the hostname policy you want to use.

5. Save the configuration.

Modifying a Hostname Rewrite Policy

To modify a hostname rewrite policy, complete the following:

1. From the DataManagement tab, select the DHCP tab, expand the Toolbar and click GridDHCPProperties.
2. In the GridDHCPProperties editor, click ToggleAdvancedMode.
3. In the IPv4DDNS -> Advanced tab, do the following in the HostnameRewritePolicy section:
   - Select a policy from the table, and then click the Edit icon.
   - In the Edit Hostname Rewrite Policy section, modify and test the policy as described in Adding and Enabling a Hostname Rewrite Policy.

**Note:** If you enable the policy at the Grid level, you can modify all information, including the policy name. If you enable the policy at the member level, you can modify any information, except for the policy name.

4. Click Save. The appliance updates the policy in the table.
5. Save the configuration.

Overriding a Grid Hostname Rewrite Policy

You can override a Grid hostname rewrite policy at the member level. To override a Grid policy, complete the following:

1. From the DataManagement tab, select the DHCP tab and click the Members tab -> member check box -> Edit icon.
2. In the Member DHCP Properties editor, click Toggle Advanced Mode.
3. In the IPv4 DDNS -> Advanced tab, click Override in the Hostname Rewrite Policy section, and then complete the following:
   - **Enable hostname rewrite policy:** Select this check box to use a hostname rewrite policy, or deselect the check box to disable the policy.
   - When you enable this feature, select a policy that you want to use from the drop-down list. Grid Manager displays all hostname rewrite policies that you have configured on the appliance in the drop-down list. After you select a policy, Grid Manager displays the policy name, valid characters, and the replacement character.

4. Save the configuration.

About the Client FQDN Option

When an IPv4 DHCP client sends DHCP DISCOVER and DHCP REQUEST messages, it can include option 81, the Client FQDN option. An IPv6 DHCP client can include option 39, the Client FQDN option, when it sends Solicit and Request messages. The Client FQDN option contains the FQDN (fully qualified domain name) of the client and instructions on whether the client or the server performs DNS updates. You can configure the appliance to replace the FQDN in the option by defining a hostname rewrite policy. For information about adding and enabling a hostname rewrite policy, see Replacing Host Names for DDNS Updates.

The DHCP server can support option 81 for IPv4 and IPv6 clients, and use the host name or FQDN that the client provides for the update. It can also allow or deny the client's request to update DNS, according to the administrative policies of your organization. The DHCP server indicates its response in the DHCP OFFER message it sends back to an IPv4 client, and in the Reply message it sends back to an IPv6 client.

Sending Updates with the FQDN Option Enabled

When you enable the DHCP server to support the FQDN option, it uses the information provided by the IPv4 or IPv6 client to update DNS as follows:

- When an IPv4 or IPv6 DHCP client sends a DHCP request with the FQDN option, it can include either its FQDN or only its host name.
  - If the request includes the FQDN, the DHCP server uses this FQDN to update DNS. You can specify a list of forward-mapping zones to be updated for IPv4 and IPv6 clients using the FQDN option. For information, see Sending Updates for DHCP Clients Using the FQDN Option.
  - If the request includes the host name, the DHCP server provides the domain name. It combines the host name of the client and the domain name to create an FQDN for the client. It then updates DNS with the FQDN it created. (You can enter the domain name in the General page of the DHCP Properties window. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients)

- When a DHCP client sends a DHCP request with its hostname, the DHCP server adds the domain name you specified to create an FQDN for the client. It then updates DNS with the FQDN it created. For information about entering the domain name, see Enabling DDNS for IPv4 and IPv6 DHCP Clients.
- When a DHCP client does not send a host name, the DHCP server provides a lease but does not update DNS. You can configure the DHCP server to generate a host name and update DNS as described in Generating Host Names for DDNS Updates.
If multiple DHCP clients specify the same FQDN or host name, the DHCP server allocates leases to the clients, but updates DNS only for
the client that first sent the request. When it tries to update DNS for the succeeding clients, the update fails.

Sending Updates from DHCP Clients or a DHCP Server

When you enable the DHCP server to support the FQDN option, you must decide if you want the DHCP server to allow clients to update DNS. If
you allow the client to update DNS, then the client updates its A or AAAA record only. The DHCP server always updates the PTR records. You
can configure the DHCP server as follows:

- The DHCP server can allow clients to update DNS when they send the request in the FQDN option. This is useful for small sites where
security is not an issue or in sites where clients move from one administrative domain to another and want to maintain the same FQDN
regardless of administrative domain.
- If you configure the DHCP server to allow clients to perform DDNS updates, you must also configure the DNS server to accept these
updates from clients. Note that multiple clients can use the same name, resulting in multiple PTR records for one client name.
- When a lease expires, the DHCP server does not delete the A or AAAA record, if it was added by the client.
- The DHCP server can refuse the DHCP client’s request to update DNS and always perform the updates itself. When the DHCP server
updates DNS, it uses the FQDN provided by the DHCP client. Select this option if your organization requires tighter control over your
network and does not allow clients to update their own records.

Do the following to configure support for the FQDN option for both IPv4 and IPv6 clients:

- Enable support for the option and specify who performs the DDNS update. For more information, see Enabling FQDN Option Support.
- Specify the DNS zones and DNS view for the updates. For more information, see Sending Updates for DHCP Clients Using the FQDN Option.

Enabling FQDN Option Support

You can configure support for the FQDN option for IPv4 and IPv6 clients at the Grid, member, network and shared network levels.

To configure support for the FQDN Option (option 81) for IPv4 and (Option 39) for IPv6:

1. **Grid:** From the Data Management tab, select the DHCP tab, expand the Toolbar and click Grid DHCP Properties. **Member:** From the Data Management tab, select the DHCP tab and click the Members tab -> member check box -> Edit icon.
   - **Network:** From the Data Management tab, select the DHCP tab and click the Networks tab -> Networks -> network check box -> Edit icon.
   - **Shared Network:** From the Data Management tab, select the DHCP tab and click the Networks tab -> Shared Networks -> shared_network check box -> Edit icon.
   - To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the IPv4 DDNS -> Advanced tab for the Grid and member, or the IPv4 DDNS -> Basic tab for the network, do the following:
   - **Option 81 Support**
     - **Enable Option 81 Support:** Select this to enable the support for option 81.
     - **DHCP server always updates DNS:** Select this to allow the DHCP server to update DNS, regardless of the requests from DHCP clients.
     - **DHCP server updates DNS if requested by client:** Select this to allow the DHCP server to update DNS only when requested by DHCP clients.

3. In the IPv6 DDNS -> Advanced tab for the Grid and member, or the IPv6 DDNS -> Basic tab for the network, do the following:
   - **FQDN Support:** Select Enable FQDN Support and select one of the following to indicate whether the DHCP server or the client performs the DDNS update.
     - **DHCP always updates DNS**
     - **DHCP updates DNS if requested by client**

4. Save the configuration and click Restart if it appears at the top of the screen.

When a lease expires, the DHCP server removes the A or AAAA records and PTR records that it updated. It does not remove any records that
the client updated.

Sending Updates for DHCP Clients Using the FQDN Option

You must specify the DNS view to be updated for each network view.

To send updates to zones for DHCP IPv4 and IPv6 clients using the FQDN option:

1. If there are multiple network views in the Grid, select a network view.
2. From the Data Management tab, select the DHCP tab, and then click Configure DDNS from the Toolbar.
3. In the DDNS Properties editor, complete the following:
   - DNS View: If a network view has more than one DNS view, this field lists the associated DNS views. From the drop-down list, select the DNS view to which the DHCP server sends DDNS updates. Otherwise, the appliance uses the default DNS view.
   - Zones to Update for Hosts Using DHCP FQDN Option: In this section, you can define forward-mapping zones to which the DHCP server sends DDNS updates for IPv4 and IPv6 DHCP clients that use the FQDN option. You must first enable support for the FQDN option before the DHCP server can send DDNS updates to these zones. By default, the DHCP server sends DDNS updates to zones using the domain name that you define for DHCP objects, such as networks and DHCP ranges. For clients using this option, the DHCP server uses the domain name defined in the option. Click the Add icon to specify a forward-mapping zone. Note that the Forward-mapping Zone Selector dialog box displays only the DNS zones that are associated with the selected DNS view. The zones you select here are written to the dhcpd.conf file and the dhcpdv6.conf file as "zone" statements with the matching TSIG key of the DNS view, so the updates are sent to the correct DNS view.
4. Save the configuration and click Restart if it appears at the top of the screen.

Configuring DDNS Update Verification

The DHCP server can handle DDNS updates differently, depending on how stringently you configure record handling. You can configure the DHCP server to update records only after passing verification. You can adjust the way DHCP handles updates so the DHCP server updates records after passing less stringent verification requirements, or without any type of verification.

To provide a measure of protection against unintentional changes of DNS data, NIOS appliances support the generation and use of TXT records, as described in IETF draft, draft-ietf-dhc-dhcp-dns-12.txt and by the ISC (Internet Systems Consortium). When DHCP updates or deletes an A or AAAA record, the corresponding TXT record is checked first to verify the authenticity of the update. The TXT record is based on a hash of the DHCID which is unique to each client, usually based in part on the MAC address or the DUID. If the client requests an update to DNS, the DHCP server first checks the TXT record to verify that it matches the client that originally inserted the record. This process provides assurance that the updates are from the same client. These security checks are based upon inserting a cryptographic hash of the DHCID (DHCP Client Identifier) into a DNS TXT RR and then verifying that value before updating. For example, a sample client update adds the following records in DNS:

<table>
<thead>
<tr>
<th>oxcart.lo0.net.</th>
<th>21600</th>
<th>IN A 172.31.1.20</th>
</tr>
</thead>
<tbody>
<tr>
<td>oxcart.lo0.net.</td>
<td>21600</td>
<td>IN TXT &quot;313ce164780d34b91486b7c489ed7467e6&quot;</td>
</tr>
<tr>
<td>20.1.31.172.in-addr.arpa.</td>
<td>21600</td>
<td>IN PTR oxcart.lo0.net.</td>
</tr>
</tbody>
</table>

However, your DNS configuration might require that the NIOS appliance handle DNS record updates differently than described in draft-ietf-dhc-dhcp-dns-12.txt. Your specific requirements might benefit from less-stringent verification of the DHCID, or might require skipping verification entirely. Verification checks might cause complications in some specific cases described below:

- **Mobility**: The TXT record is based on the DHCID unique to each client and is usually based on the MAC address or DUID of the interface. Devices such as laptops that connect to both wired and wireless networks have different MAC addresses or DUIDs and different DHCID values for each interface. In this scenario, after either one of the network interfaces inserts a DNS record, updates are allowed from that interface only. This results in a disruption of service for DDNS updates when roaming between wired and wireless networks.

- **Migration**: The second problem occurs during a migration from non-ISC based systems to ISC systems. For example, if the user is migrating from a Microsoft-based system, the clients have A or AAAA and PTR records in the DDNS updates but no TXT records. As a result, new DDNS updates fail after the migration.

- **Mixed Environments**: The final problem occurs in mixed ISC and non-ISC environments. For example, assume that both Microsoft and ISC DHCP servers update DNS records on the appliance. In a mixed environment, since the Microsoft DHCP server does not insert the TXT records, DDNS updates from ISC-based systems fail while updates from the Microsoft DHCP server are committed into the database. This behavior is applicable only when you select Standard ISC and Check TXT only DDNS update verification modes.

The NIOS appliance offers four modes to handle DDNS updates as described in Figure 21.4:

**Figure 21.4 DDNS Update Verification Mode**

<table>
<thead>
<tr>
<th>Mode</th>
<th>If a Record at Grant</th>
<th>Then TXT Record at Grant</th>
<th>Lease Grant Action</th>
<th>Lease Expire Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard ISC</td>
<td>Exists</td>
<td>Must match</td>
<td>Delete A or AAAA, TXT if exists</td>
<td>Delete PTR, Delete A or AAAA, TXT if TXT matches and no other A or AAAA RRs</td>
</tr>
<tr>
<td></td>
<td>No A or AAAA record</td>
<td>No check</td>
<td>Add A or AAAA, TXT Add PTR</td>
<td>Add A or AAAA, TXT Add PTR</td>
</tr>
</tbody>
</table>
Depending on your expected usage, you must carefully consider the various options for update verification. The following section illustrates recommendations for each verification option:

- **Standard ISC**: This method is the most stringent option for verification of updates. This is the default.
- **ISC Transitional**: This method is useful during migrations from systems that do not support the TXT record to systems that are ISC-based.
- **Check TXT only**: This method is useful for the roaming laptop scenario. The NIOS appliance checks that a TXT record exists, but does not check the value of the TXT record.
- **No TXT record**: This method should be used with caution because anyone can send DDNS updates and overwrite records. This method is useful when both ISC and non-ISC-based DHCP servers and clients are updating the same zone. Infoblox recommends that you allocate a DNS zone for this authentication method, as a precaution.

Note: In certain situations, when a DHCP lease expires, the DHCP server might remove the TXT record even if there is no A or AAAA record.

You can enable this feature at the Grid level. To configure TXT record handling on the DHCP server:

1. From the Data Management tab, select the DHCP tab, expand the Toolbar and click Grid DHCP Properties.
2. In the IPv4 DDNS -> Advanced tab or the IPv6 DDNS -> Advanced tab, select one of the following from the TXT (DHCID) Record Handling drop-down list:
   - **Check Only**: Select this check box to enable minimal checking of DDNS updates. Specifically, A or AAAA records are modified only if a TXT record exists. The NIOS appliance checks that a TXT record exists, but does not check its value.
   - **ISC**: Select this check box to enable standard ISC (Internet Systems Consortium) handling for DDNS updates. Specifically, A or AAAA records are modified or deleted only if the TXT records match. This option is the default setting on the appliance.
   - **ISC Transitional**: Select this check box to enable less stringent handling of DDNS updates. Specifically, the NIOS appliance enables you to add or modify A or AAAA records whether or not TXT records exist. It checks whether a TXT record exists and then processes the update. If the appliance does not find a TXT record, it adds the record.
   - **No TXT Record**: Select this check box to disable TXT record checking. Specifically, A or AAAA records are added, modified, or deleted whether or not the TXT records match. No TXT records are added, and existing TXT records are ignored.
3. Save the configuration and click Restart if it appears at the top of the screen.

### Configuring DNS Servers for DDNS

For security reasons, an Infoblox DNS server does not accept DDNS updates by default. You must specify the sources from which you want to allow the DNS server to receive updates. You can configure the Infoblox DNS server to receive updates from specified DHCP clients, as described in Enabling DNS Servers to Accept DDNS Updates, and to accept forwarded updates from another DNS server, as described in Forwarding Updates.

For protection against spoofed IP addresses, you can use TSIG (transaction signatures) to authenticate and verify updates.

TSIG uses the MD5 (Message Digest 5) algorithm and a shared secret key to create an HMAC (hashed message authentication code) — sometimes called a digital fingerprint — of each update. Both the DHCP server sending the update and the DNS server receiving it must share the same secret key. Also, it is important that the time stamps on the TSIG-authenticated updates and update responses be synchronized, or the participants reject them. Therefore, use an NTP server to set the time on all systems involved in TSIG authentication operations.

The TSIG key that you use can come from several places:

- You can use the key generation tool described in this section to create a new TSIG key to authenticate updates from the DHCP server.
- You can enter (copy and paste) a TSIG key that you previously generated for another purpose, such as for zone transfers.
- If the DHCP server is on a separate appliance and a TSIG key was previously generated on that appliance, you can enter (copy and paste) that TSIG key onto the local DNS server.
The TSIG key name and value that the DHCP and DNS servers use must be the same.

Note: Whether you deploy NIOS appliances in a Grid or independently, they send updates to UDP port 53. Grid members do not send updates through a VPN tunnel. Grid members do, however, authenticate updates between them using TSIG (transaction signatures) based on an internal TSIG key.

Enabling DNS Servers to Accept DDNS Updates

You can configure the Infoblox DNS server to receive updates from specified DHCP clients only. You can set this for the Grid so that the Grid members receive DDNS updates only from the specified sources. Note that you specify the IP addresses of the sources of the updates and not the actual IP addresses in the DNS records being updated.

To configure the DNS server to accept updates from the specified sources:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. Member: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon. Zones: From the Data Management tab, select the DNS tab and click the Zones tab-> dns_view -> zone check box -> Edit icon. To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the editor, click Toggle Advanced Mode, select the Updates tab.

Note: Ensure that you understand how the appliance handles match lists before you specify the list of IP sources for DDNS updates, as described in You can use the following OpenStack cloud-init template to configure an IB-V815 as a Grid Master: 3.

3. In the Allow updates from section, select one of the following:
   - None: Select this to deny DDNS updates from all DHCP clients. This is selected by default.
   - NamedACL: Select this and click SelectNamedACL to select a named ACL. Grid Manager displays the NamedACLs Selector. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this option, the appliance receives DDNS updates from the sources that have the Allow permission in the named ACL. You can click Clear to remove the selected named ACL.
   - SetofACEs: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows.
     - IPv4Address and IPv6Address: Select this to add an IPv4 address or IPv6 address. Click the Value field and enter the IP address. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.
     - IPv4Network: In the AddIPv4Network panel, complete the following, and then click Add to add the network to the list:
       - Address: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
       - Permission: Select Allow or Deny from the drop-down list.
     - IPv6Network: In the AddIPv6Network panel, complete the following, and then click Add to add the network to the list:
       - Address: Enter an IPv6 network address and select the netmask from the drop-down list.
       - Permission: Select Allow or Deny from the drop-down list.
     - TSIGKey: In the AddTSIGKey panel, complete the following, and then click Add to add the TSIG key to the list:
       - Keyname: Enter a meaningful name for the key, such as a zone name or the name of a remote name server. This name must match the name of the same TSIG key on other name servers.
       - KeyAlgorithm: Select either HMAC-MD5 or HMAC-SHA256.
       - Key Data: To use an existing TSIG key, type or paste the key in the Key Data field. Alternatively, you can select the key algorithm, select the key length from the Generate Key Data drop down list, and then click Generate Key Data to create a new key.

Note: You must enable GSS-TSIG signed updates to receive DDNS updates from TSIG key based ACEs. For information about how to enable this, see Accepting GSS-TSIG Updates.

   - AnyAddress/Network: Select this to receive DDNS updates from any IP addresses. After you have added access control entries, you can do the following:
     - Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL icon and enter a name in the Convert To Named ACL dialog box. The appliance creates a new named ACL and adds it to the Named ACL panel. Note that the ACEs you configure for this operation stay intact.
     - Reorder the list of ACEs using the up and down arrows next to the table.
     - Select an ACE and click the Edit icon to modify the entry.
     - Select an ACE and click the Delete icon to delete the entry. You can select multiple ACEs for deletion.

   - Allow GSS-TSIG signed updates: This check box is selected only if you have enabled GSS-TSIG signed updates.

4. Optionally, you can:
   - Modify an item on the list by selecting it and clicking the Edit icon.
   - Remove an item from the list by selecting it and clicking the Delete icon.
   - Move an item up or down the list. Select it and drag it to its new position, or click the up or down arrow. The appliance applies permissions to items in the order they are listed.
5. Save the configuration.

Forwarding Updates

When a secondary DNS server receives DDNS updates, it must forward the updates to the primary server because it cannot update zone data itself. In such situations, you must enable the secondary server to receive updates from the DHCP server, and then forward them to the primary DNS server.

To configure the secondary server to accept and forward updates for all zones:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. Member: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon. Zones: From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view -> zone check box -> Edit icon. To override an inherited property, click Override next to it and complete the appropriate fields.

2. In the editor, click Toggle Advanced Mode.

3. When the additional tabs appear, click the Advanced subtab of the Updates tab, and then complete the following:
   - Allow secondary name servers to forward updates: Select this check box.
   - Forward updates from: This is available only for authoritative zones. Click Add. Depending on the item that you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows:
     - **None**: Select this to deny DDNS updates from any clients. This is selected by default.
     - **Named ACL**: Select this and click Select Named ACL to select a named ACL. Grid Manager displays the Named ACLs Selecto r. Select the named ACL you want to use. If you have only one named ACL, Grid Manager automatically displays the named ACL. When you select this option, the appliance receives DDNS updates from the sources that have the Allow permission in the named ACL. You can click Clear to remove the selected named ACL.
     - **Set of ACEs**: Select this to configure individual ACEs. Click the Add icon and select one of the following from the drop-down list. Depending on the item you select, Grid Manager either adds a row for the selected item or expands the panel so you can specify additional information about the item you are adding, as follows:
       - **IPv4 Address** and **IPv6 Address**: Select this to add an IPv4 address or IPv6 address. Click the Value field and enter the IP address. The Permission column displays Allow by default. You can change it to Deny by clicking the field and selecting Deny from the drop-down list.
       - **IPv4 Network**: In the Add IPv4 Network panel, complete the following, and then click Add to add the network to the list:
         - Address: Enter an IPv4 network address and either type a netmask or move the slider to the desired netmask.
         - Permission: Select Allow or Deny from the drop-down list.
       - **IPv6 Network**: In the Add IPv6 Network panel, complete the following, and then click Add to add the network to the list:
         - Address: Enter an IPv6 network address and select the netmask from the drop-down list.
         - Permission: Select Allow or Deny from the drop-down list.
       - **TSIG Key**: In the Add TSIG Key panel, complete the following, and then click Add to add the TSIG key to the list:
         - Key name: Enter a meaningful name for the key, such as a zone name or the name of a remote name server. This name must match the name of the same TSIG key on other name servers.
         - Key Algorithm: Select either HMAC-MD5 or HMAC-SHA256.
         - Key Data: To use an existing TSIG key, type or paste the key in the Key Data field. Alternatively, you can select the key algorithm, select the key length from the Generate Key Data drop down list, and then click Generate Key Data to create a new key.

   Note: You must enable GSS-TSIG signed updates to receive DDNS updates from TSIG key based ACEs. For information about how to enable this, see Accepting GSS-TSIG Updates.

   - **Any Address/Network**: Select to allow or disallow the appliance to receive DDNS updates from any IP address. After you have added access control entries, you can do the following:
     - Select the ACEs that you want to consolidate and put into a new named ACL. Click the Create new named ACL icon and enter a name in the ConverttoNamedACL dialog box. The appliance creates a new named ACL and adds it to the NamedACL panel. Note that the ACEs you configure for this operation stay intact.
     - Reorder the list of ACEs using the up and down arrows next to the table.
     - Select an ACE and click the Edit icon to modify the entry.
     - Select an ACE and click the Delete icon to delete the entry. You can select multiple ACEs for deletion.

4. Save the configuration and click Restart if it appears at the top of the screen.

Supporting Active Directory

Active Directory™ (AD) is a distributed directory service that authenticates network users and — by working with DHCP and DNS — provides the location of and authorizes access to services running on devices in a Windows® network.

You can integrate a NIOS appliance providing DHCP and DNS services with servers running Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 with the Active Directory service installed. Assuming that you already have AD set up and it is currently in use, you can migrate DHCP and DNS services away from internal operations on the AD domain controller or from other third party DHCP and DNS systems to NIOS appliances that serve DHCP and
A NIOS appliance providing DHCP and DNS services to an AD environment can send and receive DDNS updates. In addition, a NIOS appliance can use GSS-TSIG (Generic Security Service-Transaction Signatures) authentication for DDNS updates. The basic DHCP, AD, and DNS services are shown in Figure 21.5 DHCP, Active Directory, and DNS.

Figure 21.5 DHCP, Active Directory, and DNS

Sending DDNS Updates to a DNS Server

You can configure an Infoblox DHCP server to send unauthenticated or GSS-TSIG-authenticated DDNS updates to a DNS server in an AD domain. There are no special configurations to consider when configuring a NIOS appliance to send unauthenticated DDNS updates to the DNS server. (For information about configuring DHCP, see Chapter 26, Configuring DHCP Properties, and for information on configuring the DHCP server to send DDNS updates, see Configuring DHCP for DDNS.) For information about configuring a DHCP server to send GSS-TSIG authenticated updates, see About GSS-TSIG.

About GSS-TSIG

GSS-TSIG (Generic Security Service Algorithm for Secret Key Transaction) is used to authenticate DDNS updates. It is a modified form of TSIG authentication that uses the Kerberos v5 authentication system. GSS-TSIG involves a set of client/server negotiations to establish a "security context." It makes use of a Kerberos server (running on the AD domain controller) that functions as the KDC (Kerberos Key Distribution Center) and provides session tickets and temporary session keys to users and computers within an Active Directory domain. The client and server collaboratively create and mutually verify transaction signatures on messages that they exchange. Windows 2000 server, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 all support DDNS updates using GSS-TSIG.

You can configure the appliance to accept GSS-TSIG signed DDNS updates from a single client or multiple clients that belong to different AD domains in which each domain have a unique GSS-TSIG key. You can also configure the appliance to support one or multiple GSS-TSIG keys for each Grid member. For information about how to configure GSS-TSIG for DHCP and DNS, see Configuring GSS-TSIG keys. This feature also supports HA pairs and is compatible with DNS zones that have multiple primary servers configured. For more information about HA pairs and DNS zones with multiple primary servers, see About HA Pairs and Assigning Zone Authority to Name Servers respectively.

You can upload keytab files that contain one or multiple GSS-TSIG keys and manage the keys globally. NIOS supports up to 256 GSS-TSIG keys for each member in the Grid. NIOS logs administrative changes to GSS-TSIG keys in the audit log and failures in parsing or loading the keytab files in the syslog. Note that this feature is enabled only when you have installed the DNS license.

Note: For information about GSS-TSIG, see RFC 3645, Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (G SS-TSIG).

A NIOS appliance can use GSS-TSIG authentication for DDNS updates for either one of the following:
A NIOS appliance serving DHCP can send GSS-TSIG authenticated DDNS updates to a DNS server in an AD domain or multiple AD domains whose domain controller is running Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016. The DNS server can be in the same AD domain as the DHCP server or in a different domain.

- For information about sending secure DDNS updates to a DNS server in the same domain, see bookmark1970.

- For information about sending secure DDNS updates to a DNS server in a different domain, see bookmark1976.


- For information, see Accepting GSS-TSIG-Authenticated Updates.

**Note:** A NIOS appliance cannot support both of these features at the same time.

### Kerberos Authentication for GSS-TSIG

A keytab file contains pairs of Kerberos principal names and their corresponding encryption keys. It can contain keys for a single realm or multiple realms. It is possible to infer the KDC from the principal because Windows uses uppercase AD domain names for Kerberos realm names. You must provide the principal name. The principal name may contain Kerberos realm, and the DNS servers for the domain are available for DNS name resolution. Therefore, resolving SRV _kerberos._tcp.REALM. will return the appropriate KDC. New TGTs cannot be acquired when the KDC that issues the TGT fails. If the appliance has successfully authenticated before the KDC failure, the secure updates will continue until the session key and TGT expire. The default expiration on Windows is 10 hours. If the appliance restarts or reboots, secure updates are deferred until the KDC becomes available.

Infoblox recommends restarting the DHCP service on NIOS to avoid any update failures, if the encryption key type is changed on the Microsoft server.

The following provides information about the traffic flow between the appliance and the KDC:

- Client uses keytab to get TGT for principal from KDC (AS-REQ/AS-REP).
- Client uses TGT to get session ticket from KDC (TGS-REQ/TGS-REP).
- Client uses session ticket to acquire TKEY from DNS server (TKEY/TKEY).
- Client uses TKEY to sign DNS updates (DNS-TSIG/DNS-TSIG).

The DNS server authenticates into the domain when the keytab file is generated on the KDC and its SPN (Service Principal Name) is mapped to an account. The server's private key is known to itself and to the KDC. The KDC generates the ticket and the DNS server allows the update.

Note the following when you upload multiple keytab files on the appliance:

- NIOS displays an error message and discards the keytab file if the file does not have a recognizable key, SPN, version or encryption type, and it saves the error message in the syslog.
- NIOS considers duplicate keys as invalid keys if the keys have the same SPN, version, and encryption type.
- If NIOS encounters an invalid key during an upload, it will not upload the other keys in the keytab and the operation fails. NIOS saves the warning and error message in the syslog and in Grid Manager.

### Sending Secure DDNS Updates to a DNS Server in the Same Domain

An Infoblox DHCP server can send GSS-TSIG authenticated DDNS updates to a DNS server in an AD domain whose domain controller is running Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016. The DHCP server, DNS server, and domain controller are all in the same AD domain. The process by which an Infoblox DHCP server dynamically updates resource records on a DNS server using GSS-TSIG authentication is shown in bookmark1971. In the illustration, the Kerberos Key Distribution Center (KDC) is running on an AD domain controller, which also provides DNS service.

*Figure 21.6 An Infoblox DHCP Server Sends GSS-TSIG Updates to a DNS Server*
After you enable the NIOS appliance to send GSS-TSIG authenticated updates to a DNS server, the following process occurs:

1. Kerberos – Login, and TGT and Service Ticket Assignments
   a. The Infoblox appliance automatically logs in to the AD/Kerberos server.
   b. The Kerberos server sends the appliance a TGT (ticket-granting ticket).
   c. Using the TGT, the appliance requests a service ticket for the DNS server.
   d. The Kerberos server replies with a service ticket for that server.
2. TKEY negotiations (GSS Handshake):
   a. The appliance sends the DNS server a TKEY (transaction key) request. A Transaction Key record establishes shared secret keys for use with the TSIG resource record. For more information, see RFC 2930, Secret Key Establishment for DNS (TKEY RR).
   The request includes the service ticket. The service ticket includes the appliance's principal and proposed TSIG (transaction signature) key, along with other items such as a ticket lifetime and a timestamp.
   b. The DNS server responds with a DNS server-signed TSIG, which is a "meta-record" that is never cached and never appears in zone data. A TSIG record is a signature of the update using an HMAC-MD5 hash that provides transaction-level authentication. For more information, see RFC 2845, Secret Key Transaction Authentication for DNS (TSIG).
   The two participants have established a security context.

When a DHCP client sends a request for an IP address to the DHCP server, the following occurs:

3. DHCP – IP Address and Network Parameters Assignment
   a. The DHCP client requests an IP address.
   b. The DHCP server assigns an IP address, subnet mask, gateway address, DNS server address, and a domain name.

After the appliance assigns an IP address to the DHCP client, it sends the DDNS update to the DNS server as follows:

4. DDNS – Dynamic Update of the Client's Resource Records
   c. GSS-TSIG-Authenticated DDNS Update
      1. The appliance sends an authenticated DDNS update, which may include the following resource records:
         - A or AAAA – Address record
         - PTR – Pointer record
         - TKEY – Transaction Key record
         - TSIG – TSIG record
      1. The DNS server verifies the DDNS update and allows it to complete.
      2. The DNS server sends a GSS-TSIG-authenticated response to the appliance, confirming the update.
### Configuring DHCP to Send GSS-TSIG Updates in the Same Domain

Before configuring an Infoblox DHCP server to support GSS-TSIG, you must create a user account on the Kerberos server for the appliance. Then you must export the corresponding keytab file from the Kerberos server and import it onto the NIOS appliance. Figure 21.7 illustrates the initial configuration tasks.

**Figure 21.7 Adding an Infoblox DHCP Server to an AD Environment with GSS-TSIG Support**

The Infoblox DHCP server can send GSS-TSIG-signed DDNS updates to a DNS server for one domain only, though multiple Infoblox DHCP servers can update that domain. If you want more than one Infoblox DHCP server to update a DNS domain, you can either import the same keytab file to the other Infoblox DHCP servers or generate and import a different keytab file. In a Grid, each member can update a different domain.

**Note:** For GSS-TSIG authentication to work properly, the system clock times of the Infoblox DHCP server, AD domain controller and DNS server must be synchronized. One approach is to use NTP and synchronize all three devices with the same NTP servers.

To use an AD domain controller as a Kerberos Key Distribution Center, complete the following tasks on an AD/Kerberos server:

1. Add a user account for the NIOS appliance to the AD domain controller. For information, see 
2. Generate the keytab file for the NIOS appliance account and export it from the AD domain controller to a local directory on your management system. For information, see 

To configure a NIOS appliance to support AD and send GSS-TSIG secure DDNS updates to a DNS server, complete the following tasks on a NIOS appliance:

1. Import the keytab file from your management system to the appliance and enable GSS-TSIG dynamic updates at the Grid or member level. For information, see 
2. Configure the appliance to send GSS-TSIG dynamic updates to forward-mapping and optionally, reverse-mapping zones on the DNS server. For information, see 

### Creating an AD User Account

Connect to the AD domain controller and create a user account for the NIOS appliance.
Note: The name that you enter in the User logon name is the name that you later use when exporting the keytab file. This is also the principal name. The text in the First name, Initials, Last name, and Full name fields is irrelevant to this task.

The AD domain controller automatically creates a Kerberos account for this user. Note the following:

- If you define an expiration date for the user account and you later create a new account when the first one expires, the keytab for the corresponding Kerberos account changes. At that point, you must update the keytab file on the NIOS appliance (see Enabling GSS-TSIG Authentication for DHCP). Optionally, if your security policy allows it, you can set the user account for the NIOS appliance so that it never expires.
- If the AD domain controller is running Windows Server 2003, the user account must have the DES encryption type enabled. You can enable this either in the Account tab of the AD domain controller when you create the user account or by specifying +DesOnly when you use the Ktpass tool to generate the keytab file. For instructions, see the next section, Generating and Exporting the Keytab File.

Generating and Exporting the Keytab File

You can use the Ktpass tool to generate and export the keytab file for the Kerberos account. Note that the version of the Ktpass tool that you use must match the Windows version of the domain controller. For example, if you are using a domain controller running Windows Server 2008 or Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016, you must use the Ktpass tool for Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016.


Note: The keytab file contains highly sensitive data for the NIOS appliance account. Ensure that you store and transport its contents securely.

Infoblox strongly recommends the following encryption types for compatibility purposes:

<table>
<thead>
<tr>
<th>Microsoft Windows Server</th>
<th>Export keytab</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 2000</td>
<td>Specify /crypto DES-CBC-MD5 as the export keytab.</td>
</tr>
<tr>
<td>Microsoft Windows 2003</td>
<td>Specify /crypto RC4-HMAC-NT as the export keytab.</td>
</tr>
<tr>
<td></td>
<td>Infoblox recommends that you do not use DES, but it is supported if you need it for compatibility with non-Windows systems.</td>
</tr>
<tr>
<td>Microsoft Windows 2008 and higher</td>
<td>Specify /crypto RC4-HMAC-NT as the export keytab.</td>
</tr>
<tr>
<td></td>
<td>You can also use AES, but RC4 is set by default for Windows 2008 servers.</td>
</tr>
<tr>
<td></td>
<td>Infoblox recommends that you do not use DES, but it is supported if you need it for compatibility with non-Windows systems.</td>
</tr>
</tbody>
</table>

Generating the Keytab on Windows 2000 Servers

To export the keytab file using a Microsoft Windows 2000 Resource Kit:

1. Start a command prompt.
2. Enter the following command to export the keytab file for the NIOS appliance user account:
   
   ```
   C:> ktpass -princ service_name/FQDN_instance@REALM -mapuser AD_username -pass password -out filename.keytab
   ```

Note: The values are case-sensitive.

where:

- `service_name/instance`: The AD user name for the NIOS appliance and a character string. The AD user name must match the user logon name on the AD domain controller.
- `REALM`: The Kerberos realm in uppercase. It must match the realm (or domain name) specified in the –mapuser option.
For example:
C:> ktpass -princ DNS/ns1.corpxyz.com@corpxyz.COM -mapuser ns1@corpxyz.com -pass 37Le37 -out ns1.keytab

Generating the Keytab on Windows Servers 2003

The Ktpass tool is included in the Windows Server 2003 Support Tools. To export the keytab file using a Microsoft Windows 2003 Resource Kit:

1. Start a command prompt.
2. Enter the following command to generate the keytab file for the NIOS appliance user account:

   ktpass -princ service_name/FQDN_instance@REALM -mapuser AD_username@REALM -pass password -out filename.keytab -ptype KRBR5_NT_PRINCIPAL -crypto RC4-HMAC-NT

   Note: The values are case-sensitive.

The following are some examples of keytab file:

   ktpass -princ HOST/ns1.corpxyz.com@GSS.LOCAL -mapuser gssuser@GSS.LOCAL -pass 37Le37 -out ns1.keytab -ptype krb5_nt_principal -crypto all
   ktpass -princ gssuser@GSS.LOCAL -mapuser gssuser@GSS.LOCAL -pass 37Le37 -out gssuser.keytab -ptype krb5_nt_principal -crypto all
   ktpass -princ DNS/ns1.corpxyz.com@GSS.LOCAL -mapuser jsmith@GSS.LOCAL -pass 37Le37 -out ns1.ktb -ptype KRB5_NT_PRINCIPAL -crypto des-cbc-md5 +DesOnly

   where
   -princ = Kerberos principal. Note that this parameter is case sensitive. Specifies the principal name for the host or service in this format:
   DNS/ns1.corpxyz.com@GSS.LOCAL
      • DNS = Service name in uppercase format.
      • ns1.corpxyz.com = Instance in FQDN (fully-qualified domain name) format; this is the same as the DNS name of the NIOS appliance.
      • GSS.LOCAL = The Kerberos realm in uppercase format. This must be the same as the AD domain name.
   -mapuser = Maps the Kerberos principal name to the AD user account. If you omit the account name, mapping is deleted from the specified principal. You can use ksetup without any parameters or arguments to see the current mapped settings and the default realm. Example: ksetup /mapuser <Principal> <Account>. To create an AD user account, see bookmark1974
      • jsmith = The AD user name for the NIOS appliance.
      • GSS.LOCAL = The Kerberos realm in uppercase. The realm (or domain name) must be the same as that specified in the -prin option.
   -pass = The AD user account password. The Ktpass command changes the account password to the specified value, thus incrementing the version number of the user account and the resulting keytab file.
      • 37Le37 = The password of the user account for the NIOS appliance.
   -out = The name of the keytab file that is generated.
      • ns1.ktb = The name of the keytab file
   -ptype = Sets the principal type. This must be krb5_nt_principal.
   -crypto = Specifies the encryption type. You can use the following encryption types:
      • DES-CBC-CRC = Specifies DES encryption for the account. This encryption type is used for compatibility.
      • DES-CBC-MD5 = Specifies DES encryption for the account. This encryption type adheres to the MIT implementation and is used for compatibility.
      • RC4-HMAC-NT = Specifies 128-bit RC4-HMAC encryption for the account. This is enabled by default.
   +DesOnly = Specifies DES encryption for the account.

   Note: Note that the Windows Server 2003 does not support AES encryption.

   After you execute the command to generate the keytab file, the AD domain controller displays a series of messages similar to the following to confirm that it successfully generated the keytab file:
   Targeting domain controller: ibtest-xu5md56.corpxyz.local
   Using legacy password setting method
   Successfully mapped dns/anywhere to dns.
   Key created.
   Output keytab to dns.ktb:
Generating the Keytab on Windows Servers 2008 or Windows Servers 2008 R2

To generate the keytab file using the Ktpass tool:

1. Start a command prompt.
2. Enter the following command to generate the keytab file for the NIOS appliance user account:
   
   ktpass -princ username@REALM -mapuser logon_name@REALM -pass password -out my.tab -ptype krb5_nt_principal -crypto encrypti

   Example:
   
   ktpass -princ DNS/ns1.corpxyz.com@GSS.LOCAL -mapuser jsmith@GSS.LOCAL -pass 37Le37 -out ns1.keytab -ptype krb5_nt_principal -crypto

   where:

   - **-princ** = Kerberos principal. Note that this parameter is case sensitive. Specifies the principal name for the host or service in this format:
     
     DNS/ns1.corpxyz.com@GSS.LOCAL

     - DNS = Service name in uppercase format.
     - ns1.corpxyz.com = Instance in FQDN (fully-qualified domain name) format; this is the same as the DNS name of the NIOS appliance.
     - GSS.LOCAL = The Kerberos realm in uppercase format. This must be the same as the AD domain name.

   - **-mapuser** = Maps the Kerberos principal name to the AD user account. If you omit the account name, mapping is deleted from the specified principal. You can use ksetup without any parameters or arguments to see the current mapped settings and the default realm. Example: ksetup /mapuser <Principal> <Account>. To create an AD user account, see bookmark1974.

   - jsmith = The AD user name for the NIOS appliance.
   - GSS.LOCAL = The Kerberos realm in uppercase. The realm (or domain name) must be the same as that specified in the **-princ** option.

   - **-pass** = The AD user account password. The Ktpass command changes the account password to the specified value, thus incrementing the version number of the user account and the resulting keytab file.

   - 37Le37 = The password of the user account for the NIOS appliance.

   - **-out** = The name of the keytab file that is generated.

   - ns1.ktb = The name of the keytab file

   - **-ptype** = Sets the principal type. This must be krb5_nt_principal.

   - **-crypto** = Specifies the encryption type. Note that the RC4-HMAC-NT encryption type is enabled by default. You can also use the following:
     
     - DES-CBC-CRC = Specifies DES encryption for the account. This encryption type is used for compatibility.
     - DES-CBC-MD5 = Specifies DES encryption for the account. This encryption type adheres to the MIT implementation and is used for compatibility.
     - RC4-HMAC-NT = Specifies 128-bit RC4-HMAC encryption for the account. This is enabled by default.
     - AES256-SHA1 = Specifies 256-bit AES encryption for the account.
     - AES128-SHA1 = Specifies 128-bit AES encryption for the account.
     - ALL = Specifies all of the above encryption types. Do not use this option if DES support is disabled.

   You can optionally specify the following:

   +DesOnly = Specifies DES encryption for the account. You must use this only when you use DES-CBC-MD5 for compatibility. Note that Windows 7 and Windows Server 2008 R2 do not support DES by default. However, you can enable DES on the Windows 2008 server. Include this option if you did not enable DES encryption for the account. For more information, refer to the information available in a third-party portal at:

   http://weblogic-wonders.com/weblogic/2010/11/30/windows-7-des-encryption-support-for-kerberos-authentication/

   **Note:** You must not use +Desonly with /crypto all or other non-DES encryption types.

   +setpass = Sets a new AD user account password. This is required if the +DesOnly option is specified. When you use this encryption type, you must change the user's password. Otherwise, the ticket issued for the principal becomes unusable.

   After you execute the command to generate the keytab file, the AD domain controller displays a series of messages similar to the following to confirm that it successfully generated the keytab file:

   Targeting domain controller: qacert.test.local

   Using legacy password setting method

   Successfully mapped DNS/ns1.corpxyz.com to ns1.
Generating the Keytab on Windows Servers 2012 or Windows Server 2012 R2

To generate the keytab file using the Ktpass tool:

1. Start a command prompt.
2. Enter the following command to generate the keytab file for the NIOS appliance user account:
   ktpass -princ username@REALM -mapuser logon_name@REALM -pass password -out my.tab -ptype krb5_nt_principal -crypto encryption
   
   Example:
   ktpass -princ DNS/ns1.corpxyz.com@GSS.LOCAL -mapuser jsmith@GSS.LOCAL -pass 37Le37 -out ns1.keytab -ptype krb5_nt_principal -crypto RC4-HMAC-NT
   
   where:
   -princ = Kerberos principal. Note that this parameter is case sensitive. Specifies the principal name for the host or service in this format:
   DNS/ns1.corpxyz.com@GSS.LOCAL
   -mapuser = Maps the Kerberos principal name to the AD user account. If you omit the account name, mapping is deleted from the specified principal. You can use ksetup without any parameters or arguments to see the current mapped settings and the default realm. Example: ksetup /mapuser <Principal> <Account>. To create an AD user account, see bookmark1974
   jsmith = The AD user name for the NIOS appliance.
   GSS.LOCAL = The Kerberos realm in uppercase format. The realm (or domain name) must be the same as that specified in the -princ option.
   -pass = The AD user account password. The Ktpass command changes the account password to the specified value, thus incrementing the version number of the user account and the resulting keytab file.
   37Le37 = The password of the user account for the NIOS appliance.
   -out = The name of the keytab file that is generated.
   ns1.keytab = The name of the keytab file
   -ptype = Sets the principal type. This must be krb5_nt_principal.
   -crypto = Specifies the encryption type. You can specify the following encryption types:
   - DES-CBC-CRC = Specifies DES encryption for the account. This encryption type is used for compatibility.
   - DES-CBC-MD5 = Specifies DES encryption for the account. This encryption type adheres to the MIT implementation and is used for compatibility.
   - RC4-HMAC-NT = Specifies 128-bit RC4-HMAC encryption for the account. This is enabled by default.
   - AES256-SHA1 = Specifies 256-bit AES encryption for the account.
   - AES128-SHA1 = Specifies 128-bit AES encryption for the account.
   - ALL = Specifies all of the above encryption types. Do not use this option if DES support is disabled.

After you execute the command to generate the keytab file, the AD domain controller displays a series of messages similar to the following to confirm that it successfully generated the keytab file:

Targeting domain controller: qacert.test.local

Using legacy password setting method

Successfully mapped DNS/ns1.corpxyz.com to ns1.

Key created.

Generating the Keytab on Windows Servers 2016

To generate the keytab file using the Ktpass tool:
1. Start a command prompt.
2. Enter the following command to generate the keytab file for the NIOS appliance user account:

```
ktapp -princ username@REALM -mapuser logon_name@REALM -pass password -out my.tab -ptype krb5_nt_principal -crypto encryption
```

Example:
```
ktapp -princ DNS/ns1.corpxyz.com@GSS.LOCAL -mapuser jsmith@GSS.LOCAL -pass 37Le37 -out ns1.keytab -ptype krb5_nt_principal -crypto RC4-HMAC-NT
```

where:
- **-princ** = Kerberos principal. Note that this parameter is case sensitive. Specifies the principal name for the host or service in this format: DNS/ns1.corpxyz.com@GSS.LOCAL
  - **DNS** = This is an example of the service name in uppercase format.
  - ns1.corpxyz.com = This is an example of the instance in FQDN (fully-qualified domain name) format; this is the same as the DNS name of the NIOS appliance.
  - GSS.LOCAL = This is an example of the Kerberos realm in uppercase format. This must be the same as the AD domain name.

- **-mapuser** = Maps the Kerberos principal name to the AD user account. If you omit the account name, mapping is deleted from the specified principal. You can use ksetup without any parameters or arguments to see the current settings and the default realm. Example: ksetup /mapuser <Principal> <Account>
  - jsmith = This is an example of the AD user name for the NIOS appliance.
  - GSS.LOCAL = This is an example of the Kerberos realm in uppercase. The realm (or domain name) must be the same as that specified in the **-princ** option.

- **-pass** = The AD user account password. The Ktapp command changes the account password to the specified value, thus incrementing the version number of the user account and the resulting keytab file.
  - 37Le37 = This is an example of the password of the user account for the NIOS appliance.

- **-out** = The name of the keytab file that is generated.
  - ns1.ktb = This is an example of the name of the keytab file.

- **-ptype** = Sets the principal type. This must be krb5_nt_principal.

- **-crypto** = Specifies the encryption type. You can specify the following encryption types:
  - DES-CBC-CRC = Specifies DES encryption for the account. This encryption type is used for compatibility purposes.
  - DES-CBC-MD5 = Specifies DES encryption for the account. This encryption type adheres to the MIT implementation and is used for compatibility purposes.
  - RC4-HMAC-NT = Specifies 128-bit RC4-HMAC encryption for the account. This is enabled by default.
  - AES256-SHA1 = Specifies 256-bit AES encryption for the account.
  - AES128-SHA1 = Specifies 128-bit AES encryption for the account.
  - ALL = Specifies all of the above encryption types. Do not use this option if DES support is disabled.

After you execute the command to generate the keytab file, the AD domain controller displays a series of messages similar to the following to confirm that it successfully generated the keytab file:
```
Targeting domain controller: qacert.test.local
Using legacy password setting method
Successfully mapped DNS/ns1.corpxyz.com to ns1.
Key created.
```

Output keytab to ns1.keytab:
```
Keytab version: 0x502
keysize 80 DNS/ns1.corpxyz.com@GSS.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x12 (AES256-SHA1)
keylength 32 (0xea8675d7abf13fd760a74408642fb917c6e6c9d267f5c54e5955597846f06407)
```

Creating an External Zone for GSS-TSIG Updates

For each network view, you specify the zone to be updated, the IP address of the primary DNS server for that zone, and the security method, GSS-TSIG. The zone must be in the same AD domain as the member that is sending the updates.

You can add information for a forward and reverse zone. The DHCP server updates the A record in the forward zone and the PTR record in the reverse zone.

To enable the NIOS appliance to send dynamic updates to a DNS server using GSS-TSIG for authentication:

1. If there are multiple network views in the Grid, select a network view.
2. From the **Data Management** tab, select the **DHCP** tab, expand the Toolbar and click **Configure DDNS**.
3. In the DDNS Updates to External Zones table of the **DDNS Properties** editor, click the Add icon and complete the following fields in the...
Add External DDNS Zone panel:

- **Zone Name:** Enter the name of the zone that receives the updates. You can specify both forward-mapping and reverse-mapping zones.
- **DNS Server Address:** Enter the IP address of the primary name server for that zone.
- **Security:** Select GSS-TSIG.
  - **AD Domain:** Select the AD domain associated with the keytab file.
  - **DNS Principal:** The name and domain of the DNS server receiving the DDNS updates. Note that this is not the same as the Kerberos principal you specified when you generated the keytab file.

Use the following format when you complete this field: `DNS/dns_server_fqdn@ad_domain`
- `dns_server_fqdn`: This is the FQDN of the DNS server. You can use the "dig" command to perform a DNS lookup to obtain the FQDN of the DNS server as it appears on the SOA record.
- `ad_domain`: This is the AD domain of the DNS server.

- Click **Test GSS-TSIG** to list the Grid members that are allowed to send GSS-TSIG updates to the DNS server.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Verifying the Configuration

After you configure the AD domain controller and the Infoblox DHCP server, you can view the syslog of the Infoblox DHCP server to verify if it successfully established a security context with the AD domain controller. The DHCP server displays a series of messages similar to the following:

dhcpd: Enabled GSS-TSIG for zone corpxyz. using principal jdoe/anywhere@corpxyz.LOCAL.
dhcpd: GSS-TSIG security thread has started.
dhcpd: Acquiring GSS-TSIG credential for jdoe/anywhere@corpxyz.LOCAL.
dhcpd: Acquired GSS-TSIG credential for jdoe/anywhere@corpxyz.LOCAL(good for 3568s).
dhcpd: Security context established with server 10.34.123.4 for principal[jdoe/anywhere@corpxyz.LOCAL@mailto:jdoe/anywhere@corpxyz.LOCAL] (good for 568s).
dhcpd: GSS-TSIG security update complete at 1222389338. Next update in 360s.

In addition, you can log in to the Infoblox CLI and use the show dhcp_gss_tsig CLI command to troubleshoot your configuration. For information about this command, refer to the Infoblox CLI Guide.

### Sending Secure DDNS Updates to a DNS Server in Another Domain

Domain and forest trust relationships provide clients authenticated access to resources in other domains. Some trusts are automatically created, such as the two-way, direct trust between parent and child domains in a forest. Other trusts must be created manually. Refer to the Microsoft Active Directory documentation for information on establishing trusts between domains.

Once a direct trust exists between two AD domains, a KDC from one domain can grant a referral to the KDC of the other domain. The Infoblox DHCP server can then use the referral to request access to services in the other domain. In [bookmark1977](#), the Infoblox DHCP server in the child.corpxyz.com domain needs to send GSS-TSIG authenticated DDNS updates to the DNS server in its parent domain, corpxyz.com domain. There is an automatic two-way trust between the domains because corpxyz.com domain is the parent of child.corpxyz.com domain.

![Figure 21.8 Sending Secure DDNS Updates to a DNS Server in Another Domain](image-url)
After you configure the Infoblox DHCP server and AD domain controller, the following occurs:

1. Kerberos – In Same Domain
   The Infoblox DHCP server uses the TGT (ticket-granting ticket) from the AD/Kerberos server, ad.child.corpxyz.com, to request a service ticket for DNS/ns1.corpxyz.com@corpxyz.COM. The Kerberos server replies with a referral ticket for the Kerberos server in the corpxyz.com domain, ad.corpxyz.com.

2. Kerberos — In the Other Domain
   The Infoblox DHCP server uses the referral ticket and requests a service ticket from ad.corpxyz.com for DNS/ns1.corpxyz.com@corpxyz.COM. The Kerberos server replies with a service ticket for DNS/ns1.corpxyz.com@corpxyz.COM.

3. TKEY Negotiations (GSS Handshake)
   The Infoblox DHCP server sends the DNS server ns1.corpxyz.com a TKEY (transaction key) request, which includes the service ticket. The DNS server replies with a TKEY response that includes a TSIG (transaction signature). The Infoblox appliance and the DNS server have established a security context, enabling the DHCP server to send DDNS updates to the DNS server.

Configuring DHCP to Send GSS-TSIG Updates to Another Domain

Before the DHCP server can send secure DDNS updates to a DNS server in a different domain, you must ensure that a direct trust relationship exists between the domain of the DHCP server and that of the DNS server. (For information, refer to the Active Directory documentation.) Following are the tasks to configure the AD domain controller and the Infoblox DHCP server for secure updates to another domain. All the configuration is done on the AD domain controller for the domain of the DHCP server and on the Infoblox DHCP server:

1. Complete the following tasks on the AD domain controller for the domain of the DHCP server:
   a. Add a user account for the Infoblox DHCP server. In the configuration example, the user account is ibdhcp. For information, see bookmark1974.
   b. Generate the keytab file for the Infoblox DHCP server and export it from the AD domain controller to a local directory on your management system. For the DHCP server in bookmark1977, the principal is ibdhcp/ib.child.corpxyz.com@CHILD.corpxyz.COM. For information, see bookmark1975 bookmark1975.

2. Complete the following tasks on the Infoblox DHCP server:
   a. Import the keytab file from your management system to the appliance and enable GSS-TSIG dynamic updates at the Grid or member level. For information, see Enabling GSS-TSIG Authentication for DHCP.
   b. Configure the external forward-mapping zone for the DDNS updates. Note that the DNS principal uses the domain of the DNS server, regardless of the domain of the DHCP server. For the DNS server in bookmark1977, the DNS principal is DNS/ns1.corpxyz.com@corpxyz.COM. For information, see Managing GSS-TSIG keys.

Configuration Example
Following are the steps to configure the example shown in bookmark1977:

On the AD domain controller:

1. Create a user account for the Infoblox DHCP server. The user account is ibdhcp.
2. Generate the keytab file and export it to your management system. If the domain controller is running Windows Server 2003:
   
   ktpass -princ ibdhcp@ib.child.corpxyz.com@CHILD.corpxyz.com -mapuser ibdhcp@CHILD.corpxyz.COM -pass infoblox -out ibdhcp.ktb
   
   -ptype krb5_nt_principal -crypto des-cbc-md5 +desonly

   On the Infoblox DHCP server:

1. Enable GSS-TSIG at the member level.
2. From the DHCP tab, click the Members tab -> member check box -> Edit icon.
3. In the DDNS -> Basic tab of the editor, complete the following:
   
   - Override: Select this check box.
   - DDNSUpdates: Select the EnableDDNSUpdates check box.
   - GSS-TSIG: Select Override and complete the following:
   - EnableGSS-TSIGUpdates: Select this check box.
   - DomainController: Enter ad.child.corpxyz.com. This is the KDC in the domain of the DHCP server.
   - GSS-TSIGKey: Click ManageKeytabFiles. In the KeytabFileManager dialog box, click the Add icon. Click Browse, navigate to the keytab file, select it, and then click Upload.
   
   Select the keytab file that you just uploaded. ibdhcp@ib.child.corpxyz.com@CHILD.corpxyz.COM.
   - Domain: The appliance displays the name of the domain associated with the key, which is child.corpxyz.com.
   - Click TestGSS-TSIG to list the external zones to which the Grid member can send secure DDNS updates.

4. Save the configuration and click Restart if it appears at the top of the screen.

5. Configure the external forward mapping zone, corpxyz.com.
   
   a. From the DHCP tab, expand the Toolbar and click ConfigureDDNS.
   b. In the DNS Updates to External Zones table of the DDNSProperties editor, click the Add icon and complete the following fields in the Add External DDNS Zone panel:
      
      - ZoneName: Enter corpxyz.com.
      - DNSServerAddress: Enter the IP address of the primary DNS server to which the Infoblox DHCP server sends DDNS updates. In the example, the DNS server is ns.corpxyz.com. Therefore, enter its IP address, which is 10.23.2.24.
      - Security: Select GSS-TSIG.
         
         - DNS Principal: Enter DNS/ns1.corpxyz.com@corpxyz.COM.
         - Click Test GSS-TSIG to list the Grid members that are allowed to send GSS-TSIG updates to the DNS server.

6. Save the configuration and click Restart if it appears at the top of the screen.

Sending GSS-TSIG Updates to a DNS Server in Another Forest

The Infoblox DHCP server can also send secure DDNS updates to a DNS server that belongs to a domain in another forest, as long as a forest trust exists. Refer to the Microsoft Active Directory documentation for information on establishing forest trusts.

Similar to the authentication process between domains, the authentication process between forests also uses referrals. The appliance follows the referral chain until it reaches the domain controller of the domain in which the service is located. Note that forest trusts are not transitive. For example, if the DHCP server is in forest A and the DNS server is in forest C, a direct trust must exist between forest A and forest C for the DDNS updates to succeed. Having a trust between forest A and B, and between forest B and C is not sufficient.

In bookmark1980, a trust exists between the A.Local forest and the B.Local forest. The Infoblox DHCP server in the A.Local forest needs to dynamically update the DNS server in the B.Local forest.

Figure 21.9 Sending Secure DDNS Updates to a DNS Server in Another Forest
The following authentication process occurs:

1. **Kerberos – In Same Domain**
   The Infoblox appliance uses the TGT (ticket-granting ticket) from the AD/Kerberos server, ad.child.corpxyz.com, to request a service ticket for DNS/ns1.corp200.com@CORP200.COM. The Kerberos server does not find the principal name in its domain database and after consulting the global catalog, it replies with a referral ticket for its parent domain.

2. **Kerberos — Referral Chain**
   The appliance contacts a domain controller in corpxyz.com and requests a referral to a domain controller in the corp200.com domain in B.Local Forest.
   When it receives the referral, the DHCP server contacts the domain controller and requests a service ticket for the DNS server, ns1.corp200.com. The domain controller replies with a service ticket for [DNS/ns1.corp200.com@CORP200.COM;mailto:DNS/ns1.corp200.com@CORP200.COM]

3. **TKEY Negotiations (GSS Handshake)**
   The Infoblox appliance sends the DNS server ns1.corp200.com a TKEY (transaction key) request, which includes the service ticket. The DNS server replies with a TKEY response that includes a TSIG (transaction signature). The Infoblox appliance and the DNS server have established a security context.

### Configuring DHCP to Send GSS-TSIG Updates to a Different Forest

Configuring the Infoblox DHCP server for dynamic updates to a DNS server in another forest is similar to the configuration used to send dynamic updates to another domain in the same forest. For information, see [bookmark1978](#).

### Configuring GSS-TSIG keys

You can upload keytab files that contain a single GSS-TSIG key or multiple GSS-TSIG keys on a single NIOS appliance. For each member in the Grid, you can upload up to 256 GSS-TSIG keys in a single keytab file. Trust relationships between AD domains and AD forests are not required. You can upload GSS-TSIG keys through Grid Manager or the Infoblox API. Note that only superusers can manage all GSS-TSIG keys globally on a given member through Grid Manager or the Infoblox API. Using this feature, superusers can determine the keys that belong to a particular member. You can assign multiple GSS-TSIG keys to a member and all these keys are saved in the Grid. The uploaded keys will be available in the member DNS, Grid DNS, member DHCP or Grid DHCP properties. NIOS supports the following GSS-TSIG encryption types:

- `des-cbc-crc`
- `des-cbc-md5`
- `arcfour-hmac-md5`
- `aes128-cts-hmac-sha1-96`
- `aes256-cts-hmac-sha1-96`

NIOS displays a warning message in Grid Manager and in the syslog if you upload a key that does not belong to the GSS-TSIG encryption types. For more information, see [Logging Messages](#).

### Limitations when Using Multiple GSS-TSIG keys

- You can assign SPNs belonging to different domains to a DNS member, but you cannot assign SPNs belonging to different domains to a DHCP member, although two DHCP members can update the same DNS member.
- You must ensure that the domains assigned to a DNS member are unique.
- The GSS-TSIG domain for a remote forward or remote reverse zone is single-valued. For example, if DHCP clients ABC and XYZ from Grid 1 want to send DDNS updates to Grid 2, either client ABC or XYZ will succeed.
Scheduled Upgrade

A scheduled upgrade with one or more keys in the keytab files that you have uploaded will operate the same as prior to upgrade. NIOS will parse and extract keys from the uploaded keytab file. NIOS automatically assigns these keys to the DNS member, DHCP member, Grid DHCP or Grid DNS to which the keytab file was uploaded before the upgrade. You can assign these keys to Grid members after the upgrade is complete. NIOS does not display an error message if the keys do not have an SPN with the DNS prefix, but it will record a warning message in the syslog.

Admin Permissions for Configuring GSS-TSIG keys

You can assign a key to a Grid member only if you have read permission for the kerberos key and read/write permission for the member. You can upload keys only if you have read/write permissions for kerberos keys. To remove a key that is assigned to a member, you must have read/write permission for the respective member.

Note that in the Administration -> Administrators -> Permissions tab, NIOS displays All Kerberos Keys and Kerberos Key in the Resource and Resource Type columns respectively for DHCP Admin and DNS Admin roles with default read/write permissions.

Enabling GSS-TSIG Authentication for DHCP

You can enable GSS-TSIG authentication at the Grid or member level and associate it with one or more keys of the same SPN or realm. When you enable GSS-TSIG authentication, make sure that you upload the keytab file from the Kerberos account for the Infoblox DHCP server. You can import keytab files with multiple keys to the Grid or to individual members. You can assign the uploaded keys to member DHCP or Grid DHCP. The appliance displays a warning message if you assign a GSS-TSIG key with service class "DNS" in its SPN to a DHCP member. For more information about GSS-TSIG keys, see Configuring GSS-TSIG keys.

The appliance displays an error message in the following cases:

- if you assign keys of different realms to a DHCP member or Grid DHCP.
- when you try to enable GSS-TSIG without a valid key.

The AD domain controller stores the keytab file in the directory in which you generated the keytab file. You can copy this file to a management system that connects to the NIOS appliance or launch the NIOS Grid Manager on the AD domain controller and import the keytab file to the NIOS appliance.

To enable GSS-TSIG authentication for DHCP and import keytab files:

1. **Grid:** From the Data Management tab, select the DHCP tab, expand the Toolbar and click Grid DHCP Properties. **Member:** From the Data Management tab, select the DHCP tab and click the Members tab -> member check box -> Edit icon. To override an inherited property, click Override next to it and complete the appropriate fields.

   **Standalone DHCP:** From the Data Management tab, select the DHCP tab, expand the Toolbar and click System DHCP Properties.

2. **In the IPv4 DDNS -> Basic tab or the IPv6 DDNS -> Basic tab of the editor, complete the following:**

   - **DDNS Updates:** Select Enable DDNS Updates to enable the DHCP servers in the Grid to send DDNS updates.
   - **DDNS Domain Name:** Specify the domain name of the network that the appliance uses to update DNS. For IPv4 clients, you can specify this at the network, network template, range, and range template levels. For IPv6 clients, you can specify this at the Grid, member, network, shared network, and network template levels.
   - **DDNS Update TTL:** You can set the TTL used for A record and PTR records updated by the DHCP server. The default is shown as zero. If you do not enter a value here, the appliance by default sets the TTL to half of the DHCP lease time with a maximum of 3600 seconds. For example, a lease time of 1800 seconds results in a TTL of 900 seconds, and a lease time of 86400 seconds results in a TTL of 3600 seconds.
   - **DDNS Update Method:** Select the method used by the DHCP server to send DDNS updates. You can select either Interim or Standard from the drop-down list. The default is Interim. When you select Interim, TXT record will be created for DDNS updates and when you select Standard, DHCP record will be created for DDNS updates. But in the IPv4 DDNS -> Advanced tab or the IPv6 DDNS -> Advanced tab, if you have selected No TXT Record mode for the DHCP server to use when handling DNS updates, then TXT record or DHCP record is not created for DDNS updates.
   - **If you change the DDNS update method from Interim to Standard or vice versa, then the DHCP server changes the DHCP type used from TXT record to DHCP record or vice versa as the leases are renewed.**

   This is supported for clients that acquire both IPv4 and IPv6 leases. Infoblox recommends you to configure different DDNS update method for IPv4 leases and IPv6 leases, Interim for IPv4 lease and Standard for IPv6 lease.

   - **GSS-TSIG:** Complete the following:

     - **Enable GSS-TSIG Updates:** Select this to enable the DHCP server to send GSS-TSIG authenticated DDNS updates.
     - **Manage Keystab Files:** To upload a keytab file, click Manage GSS-TSIG keys. In the Manage GSS-TSIG Keys dialog box, click the Add icon. In the Upload dialog box, click Select, navigate to the keytab file, select it, and then click Upload. You can also delete individual keys. For more information about managing GSS-TSIG keys, see Managing GSS-TSIG keys.
     - **Domain Controller:** Enter the resolvable host name or IP address of the AD domain controller that hosts the KDC for the domain.
     - **Principal:** The principal member of the key. For GSS-TSIG based DDNS updates, the SPN of the key used to carry out the update does not require the server class 'DHCP.' You can either specify an FQDN or an IP address for the <host> of an SPN.
     - **GSS-TSIGKey:** Select the name of the GSS-TSIG key from the drop-down list that you want the Grid to use. This is only available if you have uploaded a keytab file. Click the arrow beside the Add icon to either assign keys or upload and assign keys. You can either select AssignKeys or UploadAssignKeys from the drop-down list.
• Assign Keys: Select Assign Keys to select a GSS-TSIG key from the GSS-TSIG Key Selector. Click Principal, which is displayed as a hyperlink, to select it. For more information about the GSS_TSIG Key Selector, see Selecting Keys in the GSS-TSIG Key Selector.

• Upload&Assign Keys: Select Upload&Assign Keys to upload and assign keys. In the Upload dialog box, select the file and navigate to the file you want to upload. Click Upload. The appliance assigns the keys contained in the selected keytab file.

• The following are displayed in the table:
  - Version: The version of the key.
  - Encryption type: The encryption type of the key.
  - Last update: The timestamp when the key was uploaded.

• Zones this member can update securely: Click Display to list the external zones to which the Grid member can send secured DDNS updates.

• Lease Renewal Update: Select Update DNS on DHCP Lease Renewal to enable the DHCP server to update DNS when a DHCP lease is renewed.

3. Save the configuration and click Restart if it appears at the top of the screen.

Deleting GSS-TSIG keys associated with DHCP Objects

You can delete individual keys if it is not in use by the Grid or any member. To delete a key that is assigned to a member, you must have Read/Write permission for the member. To delete individual keys:

1. Grid: From the Data Management tab, select the DHCP tab, expand the Toolbar and click Grid DHCP Properties.
   Member: From the Data Management tab, select the DHCP tab and click the Members tab -> member check box -> Edit icon.
   Standalone DHCP: From the Data Management tab, select the DHCP tab, expand the Toolbar and click System DHCP Properties.

2. In the IPv4 DDNS tab or the IPv6 DDNS -> Basic tab of the editor, select keys from the list under GSS-TSIG Keys and click the Delete icon to delete keys.

Enabling GSS-TSIG Authentication for DNS

For GSS-TSIG based DDNS updates, the SPN of the key used to carry out the update must have 'DNS' in its service class. You can upload a keytab file to the Grid with multiple keys in which each key has an SPN in this format: DNS/<host>@<realm>. You can associate a DNS member or a Grid DNS with one or more keys of the same SPN or realm or of different SPN or realms. You can assign the uploaded keys to member DNS or Grid DNS, but NIOS displays an error when you try to enable GSS-TSIG without a valid key if the assigned key does not have the service class ‘DNS’ in its SPN.

To enable GSS-TSIG authentication for DNS and import keytab files:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   Member: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon. To override an inherited property, click Override next to it and complete the appropriate fields.
   Standalone DNS: From the Data Management tab, select the DNS tab, expand the Toolbar and click System DNS Properties.

2. In the GSS-TSIG -> Basic tab of the editor, complete the following:
   • GSS-TSIG: Select Enable GSS-TSIG authentication of clients to accept GSS-TSIG signed DDNS updates from clients that belong to different AD domains in which each domain has an unique GSS-TSIG key.
   • Manage Keytab Files: To upload a keytab file, click Manage GSS-TSIG keys. In the Manage GSS-TSIG Keys dialog box, click the Add icon. In the Upload dialog box, click Select, navigate to the keytab file, select it, and then click Upload. You can also delete individual keys. For more information, see Managing GSS-TSIG keys.
   • GSS-TSIG Keys: Click the arrow beside the Add icon to either assign keys or upload and assign keys. You can either select Assign Keys or Upload&Assign Keys from the drop-down list.
     • Assign Keys: Select Assign Keys to select a GSS-TSIG key from the GSS-TSIG Key Selector. Click Principal, which is displayed as a hyperlink, to select it. For more information about the GSS_TSIG Key Selector, see Selecting Keys in the GSS-TSIG Key Selector.
     • Upload&Assign Keys: Select Upload&Assign Keys to upload and assign keys. In the Upload dialog box, select the file and navigate to the file you want to upload. Click Upload. The appliance assigns keys in the uploaded file.

3. Save the configuration.

You can either specify an FQDN or an IP address for the <host> of an SPN.

• Domain: The domain name assigned to the DNS member.
• Version: The version of the key.
• Encryption type: The encryption type of the key.
• Last update: The timestamp when the key was uploaded.

DNS/<host>@<realm>

You can either specify an FQDN or an IP address for the <host> of an SPN.

• Domain: The domain name assigned to the DNS member.
• Version: The version of the key.
• Encryption type: The encryption type of the key.
• Last update: The timestamp when the key was uploaded.

NIOS sorts the data in the table based on the last updated timestamp, by default. Note that sometimes GSS-TSIG updates might stop working.
after you restart the DNS service because the appliance discards the GSS-TSIG keys, when you restart the DNS service. If this happens, wait several minutes until the Microsoft server performs another handshake using the new key.

Deleting GSS-TSIG keys associated with the DNS Objects

You can delete individual keys if it is not in use by the Grid or any member. To delete a key that is assigned to a member, you must have Read/Write permission for the member. To delete individual keys:

1. **Grid**: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
   
   **Member**: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.

2. **Standalone DNS**: From the Data Management tab, select the DNS tab, expand the Toolbar and click System DNS Properties.

3. In the GSS-TSIG -> Basic tab of the editor, select keys from the list under GSS-TSIG Keys.

4. Click the Delete icon to delete.

Logging Messages

The appliance saves the audit log entries for insert and delete operations. If you upload keys with encryption types other than the ones that NIOS supports, the appliance displays a warning message in Grid Manager and in the syslog and also it displays the encryption type as *other* in Grid Manager and in the syslog. For more information about the syslog, see Using a Syslog Server.

The appliance generates an audit log when you upload a key, assign the key to a member, remove the key associated with a member or delete a key. The audit log entries are based on each key that you have uploaded. For example, NIOS saves the following in the audit log when you upload a key:

```
2014-02-14 18:17:30.531Z [admin]: imported DNS Kerberos key for principal='DNS/infoblox.localdomain@abc.com', version=5, enctype=des-cbc-crc
```

For more information about audit logs, see Using the Audit Log. You can search Kerberos keys using the realm (domain), principal name or an encryption type.

The appliance generates a comment in the option section of the DNS configuration file for each Kerberos principal that is associated with the Grid member. These comments are for information only and it indicates the principals, their versions and encryption types that are used by the appliance.

Managing GSS-TSIG keys

You can upload a keytab file that contains one or multiple GSS-TSIG keys and delete multiple keys through the Manage GSS-TSIG Keys wizard. To manage multiple GSS-TSIG keys, complete the following:

1. From the Grid tab, select the Grid Manager tab -> Members tab, expand the Toolbar and click Manage GSS-TSIG Keys.

2. In the Manage GSS-TSIG Keys wizard, the following are displayed:
   - **Principal**: The principal name that is mapped to the keytab file.
   - **Domain**: The name of the domain that is mapped to the keytab file.
   - **Version**: The version of the key.
   - **In use**: Indicates whether the keytab file is in use or not.
   - **Members**: The members associated with the keytab file. Click the hyperlink and the Members dialog box is displayed. It displays the list of members that are associated with the keytab file.
   - **Encryption type**: The encryption type of the key.
   - **Last update**: The timestamp when the key was last uploaded.

3. Click the Upload Keytab File icon to upload a new keytab file. In the Upload dialog box, click Select and navigate to the keytab file. Click Upload to upload the file.

To delete a GSS-TSIG key, select the appropriate key and click the Delete icon.

Selecting Keys in the GSS-TSIG Key Selector

NIOS displays the keys that you have uploaded using the keytab files. You can choose a filter and an operator to view specific keys that you have uploaded. The GSS-TSIG Key Selector wizard is displayed only when you select Assign Keys in the Properties editor. For more information about how to assign keys to DNS and DHCP objects, see Enabling GSS-TSIG Authentication for DNS and Enabling GSS-TSIG Authentication for DHCP respectively.

To select a key from the GSS-TSIG Key Selector, complete the following:

1. Click Show Filter to filter the values:
   - Select a value from the drop-down list to filter your values: Domain, Encryption type, In use, Last update, Principal, and Version.
   - Select one of these operators from the drop-down list: equals, does not equal, begins with, and does not begin with.
   - Enter the value that you want to search in the text box.

   Click Hide Filter to hide the filter. Alternatively, you can enter a value in the text box for Find and click Go to search specific...
keys from the keytab files.

2. The following details are displayed in the table:

- **Principal**: The principal name that is mapped to the keytab file. Click **Principal** to assign the key to the DNS or DHCP object.
- **Domain**: The name of the domain that is mapped to the keytab file.
- **Version**: The version of the keytab file.
- **Inuse**: Indicates whether the keytab file is in use or not.
- **Members**: The members associated with the keytab file.
- **EncryptionType**: The encryption type of the key.
- **Lastupdate**: The timestamp when the key was last uploaded.

**Accepting DDNS Updates from DHCP Clients**


When adding a NIOS appliance that serves DNS to an AD environment, you must configure the AD/Kerberos server and NIOS appliance as follows—based on whether or not you want the DNS server to support DDNS updates using GSS-TSIG authentication:

- **AD/Kerberos Server**
  1. Enable zone transfers to the NIOS appliance.
  2. (For GSS-TSIG) Create a user account for the NIOS appliance that it can use for authentication.
  3. (For GSS-TSIG) Generate the keytab file of the DNS server and save it to your management system.
- **NIOS Appliance**
  4. (GSS-TSIG) Enable GSS-TSIG support.
  5. (GSS-TSIG) Import the keytab file of the DNS server from your management system to the NIOS appliance.
  7. Add a forward-mapping zone and give it a name matching the AD DNS zone whose resource records you want to import.
  8.Specify the domain controller from which the appliance can receive DDNS updates. An AD domain controller replicates its data among other domain controllers within its AD domain and among domain controllers in other domains.
  9. Import zone data from the specified domain controller.
  10. Enable the acceptance of DDNS updates from the AD domain controller and from the DHCP clients and servers whose addresses the DHCP server assigns. You can set this at the Grid, member, and zone levels.
  11. (For GSS-TSIG) Enable acceptance of GSS-TSIG DDNS updates from the AD domain controller and from the addresses that the DHCP server assigns. You can set this at the Grid, member, and zone levels.

As you can see from the above task list, adding a NIOS appliance that serves DNS to an AD environment without GSS-TSIG support involves four simple steps. To include GSS-TSIG support, there are several additional steps.

**Supporting Active Directory and Unauthenticated DDNS Updates**

Before configuring the NIOS appliance, configure the AD domain controller to permit zone transfers to the IP address of the appliance. Then on the appliance, you can do the following to configure a forward-mapping zone to support AD (Active Directory) and receive unauthenticated DDNS updates from DHCP clients, DHCP servers, and AD domain controllers.

- Create a forward-mapping zone, as described in Creating an Authoritative Forward-Mapping Zone. Give it a name that matches the AD DNS zone whose resource records you want to import.
- Specify the domain controllers from which the appliance can receive updates, as described in 4817327 4817327
- Import the zone data from the domain controller. For information, see Importing Data into Zones.
- Enable the appliance to accept DDNS updates from the DHCP clients and servers whose addresses the DHCP server assigns. You can set this at the Grid, member, and zone levels. For information, see Enabling DNS Servers to Accept DDNS Updates.

**Configuring AD Support**

You can configure a forward-mapping zone to support AD from the Active Directory wizard or from the Active Directory tab of the Authoritative Zone editor. This section describes both methods.

To configure AD support using the Active Directory wizard:
1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Configure Active Directory**. Note that from the **Zones** tab, you must select a zone before you click **Configure Active Directory**.

2. In the **Active Directory** wizard, complete the following, and then click **Next**:
   - **Select Zone**: Click this and select a zone. The name of the zone must match the name in the AD domain controller so the zone transfer from the AD domain controller to the NIOS appliance can succeed.
   - **Allow unsigned updates from Domain Controllers**: Select this option.

   If you have configured DNS resolvers in the Grid, the appliance sends DNS queries for the names and addresses of the AD domain’s domain controllers. Since the name of the zone that you selected is the same as the AD domain name on the domain controller, the appliance can then send a DNS query for the SRV records attached to the domain name. It also sends a DNS query for the A record of each domain controller to determine its IP address. The query results are listed in the next panel.

3. You can edit the list of domain controllers, if necessary. Click **Next** to proceed to the next step.
   - To add a domain controller, click the Add icon and specify the IP address.
   - To delete a domain controller from the list, select it and click the Delete icon.

4. Complete the following:
   - **Do you want to create underscore zones to hold the records added by the Domain Controllers?**
     - This option allows the appliance to create the following subzones that the DNS server must have to answer AD-related DNS queries:
       - _msdcs_.zone
       - _sites_.zone
       - _tcp_.zone
       - _udp_.zone
       - domaindnszones.zone
       - forestdnszones.zone
     - Note that these zones are automatically generated. You cannot edit these zones or import data into them. They cannot be modified, thus providing protection against forged updates.

5. Save the configuration and click **Restart** if it appears at the top of the screen.

To configure AD support using the **Authoritative Zone** editor:

1. From the **Data Management** tab, select the **DNS** tab -> **Zones** tab -> **zone** check box -> **Edit** icon.
2. In the **Authoritative Zone** editor, select the **Active Directory** tab and do the following:
   - **Allow unsigned updates from these Domain Controllers**: Select this check box and specify the AD domain controllers from which the appliance can receive DDNS updates.
   - **Automatically create underscore zones**: Select this check box to automatically create the subzones.
3. Save the configuration and click **Restart** if it appears at the top of the screen.

You can then import zone data, as described in **Importing Data into Zones**.

**Accepting GSS-TSIG-Authenticated Updates**


**Note**: For explanations of the alphanumerically notated steps in **bookmark1997**, see the section following the illustration.

---

**Figure 21.10 Authenticating DDNS Updates with GSS-TSIG**
1. DHCP – IP Address and Network Parameters Assignment
   a. The DHCP client requests an IP address.
   b. The DHCP server assigns an IP address, subnet mask, gateway address, and a DNS server address.

2. Active Directory – Computer and User Logins
   a. The computer sends a DNS request to locate the AD domain controller, and then logs in to the domain controller.
   b. The user manually logs in to a domain.

3. DNS – Query for the Kerberos Server
   a. The computer (or client) automatically sends a query for kerberos._udp.dc_msdcs.dom_name_ to the DNS server whose IP address it received through DHCP.
   b. The NIOS appliance replies with the name of the Kerberos server.

4. Kerberos – Login, and TGT and Service Ticket Assignments
   a. The client automatically logs in to the Kerberos server.
   b. The Kerberos server sends the client a TGT (ticket-granting ticket).
   c. Using the TGT, the AD member requests a service ticket for the DNS server.
   d. The Kerberos server replies with a service ticket for that server.

5. DDNS – Dynamic Update of the Client’s Resource Records
   a. Unauthenticated DDNS Update Attempt (Refused)
i. The client sends an unauthenticated DDNS update.
ii. The DNS server refuses the update.

b. TKEY negotiations (GSS Handshake):
   i. The client sends the DNS server a TKEY (transaction key) request. A Transaction Key record establishes shared secret keys for use with the TSIG resource record. For more information, see RFC2930, Secret Key Establishment for DNS (TKEYRR).
      The request includes the service ticket. The service ticket includes the appliance’s principal and proposed TSIG (transaction signature) key, along with other items such as a ticket lifetime and a timestamp.
   ii. The DNS server responds with a DNS server-signed TSIG, which is a “meta-record” that is never cached and never appears in zone data. A TSIG record is a signature of the update using an HMAC-MD5 hash that provides transaction-level authentication. For more information, see RFC2845, Secret Key Transaction Authentication for DNS (TSIG).

The two participants have established a security context.

c. GSS-TSIG-Authenticated DDNS Update (Accepted)
   i. The client sends an authenticated DDNS update, which includes the following resource records:
      - A – Address record
      - PTR – Pointer record
      - TKEY – Transaction Key record
      - TSIG – TSIG record
   ii. The DNS server authenticates the DDNS update and processes it.
   iii. The DNS server sends a GSS-TSIG-authenticated response to the AD member, confirming the update.

**Note:** For GSS-TSIG authentication to work properly, the system clock times of the Infoblox DHCP server, AD domain controller and DNS server must be synchronized. One approach is to use NTP and synchronize all three devices with the same NTP servers.

**Configuring DNS to Receive GSS-TSIG Updates**


*Figure 21.11 Adding a NIOS Appliance to an AD Environment with GSS-TSIG Support*
On an already functioning AD domain controller:

1. Enable zone transfers to the NIOS appliance.
2. Add a user account for the NIOS appliance serving DNS. A corresponding account on the Kerberos server is automatically created. For information, see bookmark2000.
3. Export the keytab file for the NIOS appliance account from the Kerberos server to a local directory on your management system. For information, see bookmark2001.

On an Infoblox appliance:

1. Import the keytab file from your management system to the Infoblox appliance and enable GSS-TSIG authentication on the appliance. For information, see bookmark2002 bookmark2002
2. Configure a forward-mapping zone with the same name as the AD zone. For information, see Creating an Authoritative Forward-Mapping Zone.
3. (Optional) Create a reverse-mapping zone for the network address space that corresponds to the domain name space in the forward-mapping zone. For information, see Creating an Authoritative Reverse-Mapping Zone.
4. Import the zone data from the AD domain controller. For information, see Importing Zone Data.
5. Enable the acceptance of GSS-TSIG-signed updates from the AD controller and from the DHCP clients and servers whose addresses the DHCP server assigns. For information, see bookmark2003.

Creating an AD User Account

Connect to the AD domain controller and create a user account for the NIOS appliance.

Note: The name you enter in the User logon name is the name that you later use when exporting the keytab file. This is also the principal name. The text in the First name, Initials, Last name, and Full name fields is irrelevant to this task.

The AD domain controller automatically creates a Kerberos account for this user with an accompanying keytab. Note the following:

- If you define an expiration date for the user account and you later create a new account when the first one expires, the keytab for the corresponding Kerberos account changes. At that point, you must update the keytab file on the NIOS appliance (see Generating and Exporting the Keytab File and bookmark2002 bookmark2002). Optionally, if your security policy allows it, you can set the user account for the
NIOS appliance so that it never expires.  
  • If the AD domain controller is running Windows Server 2003, the user account must have the DES encryption type enabled. You can enable this either in the Account tab when you create the user account or by specifying mantleDesOnly when you use the Ktpass tool to generate the keytab file.

Generating and Exporting the Keytab File

You can generate and export the keytab file for the Kerberos account by using the Ktpass tool. Note that the version of the Ktpass tool that you use must match the Windows version of the domain controller. For example, if you are using a domain controller running Windows Server 2008 or Windows Server 2008 R2, you must use the Ktpass tool for Windows Server 2008 or Windows Server 2008 R2. You enter different commands for generating and exporting the keytab file, depending on whether you are generating the keytab file from a server running Microsoft Windows 2000, Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2.

Generating the Keytab on Windows 2000

To export the keytab file using a Microsoft Windows 2000 Resource Kit:

1. Start a command prompt.
2. Enter the following command to export the keytab file for the NIOS appliance user account:

   ```
   C:> ktpass -princ <service_name>/FQDN_instance@REALM -mapuser AD_username -pass password -out filename.keytab
   ```

   For example:
   ```
   C:> ktpass -princ DNS/ns1.corpxyz.com@corpxyz.COM -mapuser ns1@corpxyz.com -pass 37Le37 -out ns1.keytab
   ```

Generating the Keytab on Windows Server 2003

The Ktpass tool is included in the Windows Server 2003 Support Tools. To export the keytab file using a Microsoft Windows 2003 Resource Kit:

1. Start a command prompt.
2. Enter the following command to export the keytab file for the NIOS appliance user account:

   ```
   ktpass -princ DNS/FQDN_instance@REALM -mapuser AD_username -pass password -out filename.keytab
   ```

   For example:
   ```
   ktpass -princ DNS/ns1.corpxyz.com@corpxyz.COM -mapuser ns1@corpxyz.com -pass 37Le37 -out ns1.keytab -ptype KRB5_NT_PRINCIPAL -crypto des-cbc-md5 +DesOnly
   ```

   where:
   - **-princ** = Kerberos principal
   - **DNS** = Service name in uppercase format
   - **ns1.corpxyz.com** = Instance in FQDN (fully-qualified domain name) format; this is the same as the DNS name of the NIOS appliance
   - **corpxyz.COM** = The Kerberos realm in uppercase format; this must be the same as the AD domain name
   - **-mapuser** = Maps the Kerberos principal name to the AD user account
   - **ns1@corpxyz.com** = The AD user name for the NIOS appliance
   - **-pass** = The AD user account password
   - **37Le37** = The password of the user account for the NIOS appliance
   - **-out** = Exports the keytab file
   - **ns1.keytab** = The name of the keytab file
   - **-ptype** = Sets the principal type. This must be krb5_nt_principal.
   - **-crypto** = Specifies the encryption type. This must be des-cbc-md5.
   - **+DesOnly** = Specifies DES encryption for the account. Include this if you did not enable DES encryption for the account.

Generating the Keytab on Windows Server 2008/Windows Server 2008 R2

A Windows Server 2008 or Windows Server 2008 R2 domain controller allows you to generate a keytab file with multiple keys for one principal. The Infoblox DNS server accepts GSS-TSIG updates from DHCP clients that provide a Kerberos ticket for any of the keys in its configured keytab. To generate the keytab file using the Ktpass tool:

1. Start a command prompt.
2. Enter the following command to export the keytab file for the NIOS appliance user account:

   ```
   ktpass -princ DNS/FQDN_instance@REALM -mapuser AD_username -pass password -out filename.keytab
   ```

   For example:
   ```
   ktpass -princ DNS/ns1.corpxyz.com@corpxyz.COM -mapuser ns1@corpxyz.com -pass 37Le37 -crypto encryption
   ```
Modifying an AD User Account

To change any AD user account information (login, password, etc):

1. Remove the previous user account from AD.
2. Create a new user for GSS-TSIG mapping.
4. Import the keytab file to the DNS server.

Importing the Keytab File and Enabling GSS-TSIG Authentication

Before you can enable GSS-TSIG authentication, you must import the keytab file from the Kerberos account for the NIOS appliance. To import the keytab file:

1. From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
2. In the Member DNS Properties editor, click Toggle Expert Mode.
3. When the additional tabs appear, click GSS-TSIG and do the following:

   If a principal name and version number are listed, there is a keytab file loaded on the appliance. Compare this information with that for the NIOS appliance account on the Kerberos server to make sure that they match. If there is no keytab file on the NIOS appliance or if the loaded keytab file does not match that on the Kerberos server, you must load the correct keytab file

   - Click Upload, click Browse to navigate to the keytab file, and then click Upload.
   - EnableGSS-TSIGAuthenticationofClients: Select this check box.

4. Save the configuration and click Restart if it appears at the top of the screen.

Each time you export a keytab file from a Kerberos server running on Windows Server 2003, the version number of the keytab file increases incrementally. Because the version number on the keytab file that you import to the NIOS appliance must match the version that is in use on the Kerberos server, you should select the last keytab file that is exported from the Kerberos server if you have exported multiple keytab files. (A
Kerberos server running on Windows 2000 does not increase the version number of keytab files with each export.)

Accepting GSS-TSIG Updates

You can allow a Grid or specific members or zones to accept GSS-TSIG signed updates from domain controllers and DHCP clients and servers, as follows:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties.
2. Member: From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon.
3. Zone: From the Data Management tab, select the DNS tab -> Zones tab -> zone check box -> Edit icon.

To override an inherited property, click Override next to it and complete the appropriate fields.

2. Select the Updates tab and do the following in the Basic subtab:
   - Allow GSS-TSIG signed updates: Select this option.

3. Save the configuration and click Restart if it appears at the top of the screen.

You can then use the Active Directory wizard or navigate to the Active Directory tab of the Authoritative Zone editor to enable the appliance to create underscore zones for the records hosted by domain controllers and to allow GSS-TSIG signed updates to the underscore zones.

To use the Active Directory wizard:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Configure Active Directory.
2. In the Configure Active Directory wizard, complete the following, and then click Next:
   - Select Zone: Click this and select a zone. The name of the zone must match the name in the AD domain controller so the zone transfer from the AD domain controller to the NIOS appliance can succeed.
   - Allow GSS-TSIG-signed (secure) updates from Domain Controllers: Select this option.
3. Complete the following:
   - Do you want to create underscore zones to hold the records added by the Domain Controllers?
     This option allows the appliance to create the following subzones that the DNS server must have to answer AD-related DNS queries:
     - _msdcs.zone
     - _sites.zone
     - _tcp.zone
     - _udp.zone
     - domaindnszones.zone 
     - forestdnszones.zone 
     Note that these zones are automatically generated. You cannot edit these zones or import data into them.
   - Allow GSS-TSIG-signed updates to underscore zones: Select this check box to allow underscore zones to accept GSS-TSIG signed updates.

4. Save the configuration and click Restart if it appears at the top of the screen.

To use the Authoritative Zone editor:

1. From the DataManagement tab, select the DNS tab -> Zones tab -> zone check box -> Edit icon.
2. In the AuthoritativeZone editor, select the ActiveDirectory tab and do the following:
   - Allow unsigned updates from these Domain Controllers: Clear this check box.
   - Automatically create underscore zones: (select)
     This option automatically creates the following subzones that the DNS server must have to answer AD-related DNS queries:
     - _msdcs.zone
     - _sites.zone
     - _tcp.zone
     - _udp.zone
     - domaindnszones.zone 
     - forestdnszones.zone 
     Note that these zones are automatically generated and cannot be manually edited.
   - Allow GSS-TSIG-signed updates to underscore zones: Select this check box to allow underscore zones to accept GSS-TSIG signed updates.

3. Save the configuration and click Restart if it appears at the top of the screen.

Secure Dynamic Updates

The secure dynamic updates feature provides several methods to restrict dynamic DNS updates to certain records. This includes:

- Restrictions for updates to statics records. For more information, see 4819980
- Restrictions for updates to records marked as protected. For more information, see 4819980 4819980.
- Restrictions based on GSS-TSIG principal authentication. For more information, see 4819980 4819980.
- Restrictions based on FQDN patterns. For more information, see 4819980.
Only static and dynamic record source type support secure dynamic updates. You can see the record source type in the Resource Record Viewer. The following table shows which type of secure dynamic updates is applicable to different record source types.

**Table 21.1 Secure Dynamic Update Types**

<table>
<thead>
<tr>
<th>Secure Dynamic Update Type</th>
<th>Record Source Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrictions for updates to statics records</td>
<td>Static</td>
</tr>
<tr>
<td>Restrictions for updates to protected records</td>
<td>Static, dynamic</td>
</tr>
<tr>
<td>Restrictions based on GSS-TSIG principal authentication</td>
<td>Dynamic</td>
</tr>
<tr>
<td>Restrictions based on FQDN patterns</td>
<td>Static, dynamic</td>
</tr>
</tbody>
</table>

Sometimes when the updating record has the same data as the existing record, you may need to initialize the record creation timestamp to avoid unwanted DNS record scavenging. For more information, see [Forcing Creation Timestamp Initialization for Unchanged Records](#).

Failed attempts to dynamically update secured records are recorded in the NIOS syslog. You can view it, as described in [Viewing the Syslog](#) and [Searching in the Syslog](#).

You can use Smart Folders to organize data by record source, principal, or protection state. For more information, see [Chapter 3, Smart Folders](#).

In addition, you can use Global Search to search for records by principal name. For more information, see [Using Global Search](#).

**Note:** To use the secure dynamic updates feature, you must have a DNS license installed in the Grid Manager.

### Restricting Updates to Static Records

This method prevents updates to all RRsets containing static records at once in the Grid, DNS view, or zone. To prevent updates to specific static records, see [4819980](#).

**Note:** When you upgrade from a previous NIOS version to NIOS 7.3 or later, all dynamic updated records are labelled as static records if you enable the Secure Dynamic Updates feature. Infoblox suggests that you enable this feature only after all records are changed to Dynamic. NIOS tags the RRsets that are not auto-generated as static records.

To restrict updates to all static records in the Grid, DNS view, or zone:

1. In the Grid DNS, view, or zone properties, click **Updates -> Advanced**.
2. To override the inherited properties, click **Override**.
3. Under **Secure Dynamic Updates**, select **Prevent dynamic updates to RRsets containing static records**.
4. Click **Save & Close**.

### Restricting Updates to Protected Records

You can restrict updates to the records of your choice, by marking them as protected. You can do this for both static and dynamic records. The Resource Record Viewer displays the protection status of the records in the Protected column: Yes or No.

You can protect the following record types:

- A record
- AAAA record
- CNAME record
- DNAME record
- MX record
- NAPTR record
- PTR record
- SRV record
- TXT record
- Host record

For all the above mentioned records except the host record, you can change the type from static to dynamic and back, if required.

To restrict updates to protected records:

1. In the DNS Resource Records viewer, select a record or multiple records.
2. In the Toolbar, select **Protect Records -> Enable Protection**.
   
   Or
   
   In the properties dialog for a record, click **Updates**, select the **Protected** check box, and then click **Save & Close**.

3. Enable updates prevention at the corresponding level:
Restricting Updates Based on GSS-TSIG Principal Authentication

This method implies tracking the Kerberos GSS-TSIG principal that created a record and restricting DDNS updates attempted by a different GSS-TSIG principal on this record.

The Resource Record Viewer displays the GSS-TSIG authentication information in the Principal column: it displays the principal name if the client that created the record is authenticated and the principal is tracked.

The tracked principal is also displayed in the record properties. You can change the principal associated to a record by clicking Select Principal in the record properties and specifying the required principal.

Additionally, you can use dynamic update groups to manage the allowed principals. For more information, see 4819980 4819980.

To restrict updates based on GSS-TSIG principal authentication:

1. In the Grid DNS, view, or zone properties, click Updates -> Advanced.
2. To override the inherited properties, click Override.
3. Under Secure Dynamic Updates, select Track the GSS-TSIG principals that create dynamic records.

Note: For this option to work, ensure that you have selected Enable GSS-TSIG authentication of clients in the GSS-TSIG properties of the Grid or the corresponding zone or view.

4. Select Require the appropriate GSS-TSIG principal to update RRsets that track principals.
5. Optionally, specify an active dynamic update group.
6. Click Save & Close.

About Dynamic Update Groups

In some cases, for example, in DHCP failover associations, you need to allow different GSS-TSIG principals to update each other’s records. To that end, you can join multiple principals into clusters, where all principals are considered as equivalent and therefore can update affected records without being their originators. You can join multiple clusters into a dynamic update group. The clusters within a group, however, are not considered equivalent and cannot update each other’s records.

When you have several dynamic update groups defined, you can assign different groups to be active for the Grid, a DNS view, or a zone as described in 4819980. If no group is assigned, then no principals are considered to be equivalent.

For information on how to add dynamic update groups and clusters, see 4819980.

Note: Viewing and modifying the configuration of a dynamic update group requires Grid DNS permissions. Selecting a group as active for the Grid, a view, or a zone requires read permission on the Grid DNS, as well as write permission on the object being modified.

Managing Dynamic Update Groups and Clusters

To add a dynamic update group:

1. In Data Management -> DNS, expand the Toolbar and click Manage Dynamic Update Groups.
2. Click the Add icon.
4. Specify the group name.
5. Optionally, provide a comment.
6. Click Save and Close. Proceed to adding clusters to the group as described below.

To add a cluster:

1. In the Manage Dynamic Update Groups window, click the Add icon.
2. Select Add Cluster.
3. Select the dynamic update group in which you want to include the cluster.
4. Specify the cluster name.
5. Optionally, provide a comment.
6. Click Save and Close.
7. To add principals to the cluster, select the cluster in the Manage Dynamic Update Groups window and click the Add icon. A principal can appear in multiple clusters.
8. Select one of the following:
   - AddPrincipal: This adds a new row in the table. Specify the principal name in the row.
   - SelectPrincipal: This opens the Principal Selector dialog. Select the required principal from the list.
9. Click Close.

To edit or delete a group, cluster, or principal, select it in the Manage Dynamic Update Groups window, and click the corresponding icon. You can also export data about dynamic update groups, their clusters, and principals in the Infoblox CSV Import format by clicking the Export icon in the Manage Dynamic Update Groups window. For more information, see Exporting Data to Files.

Restricting Updates Based on FQDN Patterns

This implies defining FQDN patterns for domain names which prevents DDNS updates to matching FQDNs. To restrict updates based on FQDN patterns:

1. In the Grid DNS, view, or zone properties, click Updates -> Advanced.
2. To override the inherited properties, click Override.
3. Under Dynamic Update Patterns, select Prevent dynamic updates to FQDNs matching these patterns and specify patterns:
   - To add an FQDN pattern, click the Add icon and specify a pattern in the new table row.

   **Note:** Use the DNS Traffic Control LBDN wild cards to specify FQDN patterns. For more information, see Configuring LBDN Patterns.

   - To delete an FQDN pattern, select the check box next to the pattern and click the Delete icon.

4. Click Save & Close.

Forcing Creation Timestamp Initialization for Unchanged Records

If the attributes of a resource record do not change in the result of a DDNS update, Grid Manager ignores the update and the record’s creation timestamp remains the same. This may cause valid records with outdated timestamp to be removed during DNS scavenging. To avoid this, you can set the record creation time to be modified even when the record data do not change at DDNS update. You can do this for the whole Grid, or for a specific DNS view or authoritative zone.

To force the creation timestamp initialization for unchanged resource records:

1. Open the Grid DNS Properties, DNS View Properties, or Authoritative Zone Properties editor.
2. For a DNS view or authoritative zone, click Override.
3. Select Modify creation time even when resource record data is unchanged.
4. Click Restart in the Grid Manager’s system messages banner for the setting to take effect.

For information about DNS scavenging, see DNS Record Scavenging.

Chapter 22 DNSSEC

This chapter provides general information about DNSSEC. The topics in this chapter include:

- About DNSSEC
  - DNSSEC Resource Records
  - DNSKEY Resource Records
  - RRSIG Resource Records
  - NSEC/NSEC3 Resource Records
  - NSEC3PARAM Resource Records
  - DS Resource Records
- Configuring DNSSEC on a Grid
  - Grid Master as Primary Server
- Enabling DNSSEC
- Setting DNSSEC Parameters
  - About the DNSKEY Algorithm
  - About Key Rollovers
  - RRSIG Signatures
  - Configuring DNSSEC Parameters
  - Applying the Algorithm Changes
  - Deleting the DNSSEC Keys Associated with a Zone
- Signing a Zone
  - Managing Signed Zones
  - Importing a Keyset
  - Exporting Trust Anchors
  - Checking Key-Signing Keys
  - Rolling Key-Signing Keys
  - Rolling Zone-Signing Keys
About DNSSEC

DNSSEC (DNS Security Extensions) provides mechanisms for authenticating the source of DNS data and ensuring its integrity. It protects DNS data from certain attacks, such as man-in-the-middle attacks and cache poisoning. A man-in-the-middle attack occurs when an attacker intercepts responses to queries and inserts false records. Cache poisoning can occur when a client accepts maliciously created data. DNSSEC helps you avoid such attacks on your networks.

DNSSEC provides changes to the DNS protocol and additional resource records (RRs) as described in the following RFCs:

- RFC 4033, DNS Security Introduction and Requirements
- RFC 4034, Resource Records for the DNS Security Extensions
- RFC 4035, DNSSEC Protocol Modifications
- RFC 4641, DNSSEC Operational Practices
- RFC 4956, DNS Security (DNSSEC) Opt-In
- RFC 4986, Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover
- RFC 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
- RFC 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC

DNSSEC uses public key cryptography to authenticate the source of DNS responses and to ensure that DNS responses were not modified during transit. Public key cryptography uses an asymmetric key algorithm. With asymmetric keys, one key is used to encrypt data that was encrypted using the other key.

In DNSSEC, the primary name server of a zone generates at least one public/private key pair. It "signs" each data set in the zone by running it through a one-way hash, and then encrypting the hash value with the private key. The public key is stored in an RR type introduced by DNSSEC, the DNSKEY RR. Resolvers use the DNSKEY record to decrypt the hash value. If the hash values match, then the resolver is assured of the authenticity of the message.

In addition to the DNSKEY record, DNSSEC also introduces new RRs which DNS servers can use to authenticate the non-existence of servers, zones, or resource records. For information about the DNSSEC resource records, see DNSSEC Resource Records.

DNSSEC uses the EDNSO message extension. Resolvers include the EDNS OPT pseudo-RR with the DO (DNSSEC OK) bit set to indicate that they are requesting DNSSEC records. A DNS client or resolver sets the EDNS DO bit when it sends a query for data in a signed zone. When the DNS server receives such a query, it includes the additional DNSSEC records in its response, according to the DNSSEC standard rules. In addition, because DNSSEC messages are often large, the EDNSO message extension also provides mechanisms for handling larger DNS UDP messages. For information about EDNS0, refer to RFC 2671, Extension Mechanisms for DNS (EDNS0). For information about the DO bit, refer to RFC 3225, Indicating Resolver Support of DNSSEC.

**WARNING:** Note that when you disable EDNS0 on the appliance, all outgoing DNSSEC queries to zones within trusted anchors will fail even if DNSSEC validation is enabled. To ensure that DNSSEC functions properly, do not disable EDNS0 on the appliance. For more information, see Using Extension Mechanisms for DNS (EDNS0).

DNSSEC also supports new data in the packet header, the CD (Checking Disabled) bit and the AD (Authenticated Data) bit. The CD bit is used by resolvers in their DNS queries and the AD bit is used by recursive name servers in their responses to queries.

A resolver can set the CD bit in its query to indicate that the name server should not validate the DNS response and that the resolver takes responsibility for validating the DNS data it receives.

A name server that has successfully validated the data in a DNS response sets the AD (Authenticated Data) bit in the message header to indicate that all resource records in its response have been validated and are authentic. Note that unless the connection between the DNS server and client has been secured, such as through TSIG, the client cannot rely on the AD bit to indicate valid data. The data could have been changed in transit between the server and client. Resolvers can trust a response with the AD bit set only if their communication channel is secure.

You can also configure the NIOS appliance to always apply RPZ policies, DNS blacklists, or NXDOMAIN rules to DNS responses, regardless of
whether the queries request DNSSEC data. For more information about how to configure this, see Applying Policies and Rules to DNS Queries th at Request DNSSEC Data. For information about RPZ policies, DNS blacklists, and NXDOMAIN rules, see their respective sections in this guide.

DNSSEC Resource Records

Following are the DNSSEC RR types:

- DNS Public Key (DNSKEY) resource records — For information, see DNSKEY Resource Records.
- Resource Record Signature (RRSIG) records — For information, see RRSIG Resource Records.
- Next Secure (NSEC/NSEC3) records — For information, see NSEC/NSEC3 Resource Records.
- NSEC3PARAM records — For information, see NSEC3PARAM Resource Records.
- Delegation Signer (DS) resource records — For information, see DS Resource Records.

For detailed information about each RR, refer to RFC 4034, Resource Records for the DNS Security Extensions and RFC 5155, DNS Security (D NSSEC) Hashed Authenticated Denial of Existence.

Note: The appliance supports IDNs for DNSKEY records, DS records, NSEC records, NSEC3PARAM records, and RRSIG records.

DNSKEY Resource Records

When an authoritative name server digitally signs a zone, it typically generates two key pairs, a zone-signing key (ZSK) pair and a key-signing key (KSK) pair. The name server uses the private key of the ZSK pair to sign each RRset in a zone. (An RRset is a group of resource records that are of the same owner, class, and type.) It stores the public key of the ZSK pair in a DNSKEY record. The name server then uses the private key of the KSK pair to sign all DNSKEY records, including its own, and stores the corresponding public key in another DNSKEY record. As a result, a zone typically has two DNSKEY records; a DNSKEY record that holds the public key of the ZSK pair, and another DNSKEY record for the public key of the KSK pair.

Note: For the remainder of this chapter, the DNSKEY record that holds the public key of the ZSK pair is referred to as the ZSK and the DNSKEY record that holds the public key of the KSK is referred to as the KSK.

The purpose of the KSK is two-fold. First, it is referenced in the Delegation Signer (DS) RR that is stored in a parent zone. The DS record is used to authenticate the KSK of the child zone, so a resolver can establish a chain of trust from the parent zone to its child zone. (For more information about the DS RR, see DS Resource Records).

Second, if a zone does not have a chain of trust from a parent zone, security aware resolvers can configure the KSK as a trust anchor; that is, the starting point from which it can build a chain of trust from that zone to its child zones.

Note that though the two key pairs, KSK and ZSK, are used in most DNSSEC environments, their use is not required by the RFCs. A zone administrator can use a single private/public key pair to sign all zone data. (Note that Infoblox appliances require two key pairs.)

Following is an example of a DNSKEY RR:

corpxyz.com 1299000 IN DNSKEY 257 3 5 20131231259593hizsoggTqlKeVuG8bAchP8dq 4V5ymXsBSczueQWdjJCBsQIb7V95k0APmx ZBwMqE07xxa0eTwpqozd6E0V0zWWWhlmw 17xh0Jzxm6m71PF14av1Kq4l3Fy03693[Chylm8sMT 0ENs0IEAw7isvL2W24cE=

Owner Name

TTL

Class

RR Type

Flags Field

Protocol

Algorithm

Public Key

The first four fields specify the domain name of the zone that owns the key, the resource record TTL, class, and RR type. The succeeding fields are:

- Flags Field: In its wire format, this field is two bytes long. (The wire format is used in DNS queries and responses.) Bits 0 through 6 and 8 through 14 are reserved, and have a value of 0. Bit 7 indicates if the record holds a DNS zone key. Bit 15 is the Secure Entry Point (SEP) flag, which serves as a hint that indicates whether the DNSKEY record contains a ZSK or a KSK, as described in RFC 3757, DNSKEY SEP Flag. Zone administrators typically set the SEP flag of a DNSKEY record of a zone when it contains the KSK, to indicate that it can be used as a trust anchor. However, a DNSKEY record that does not have the SEP flag set can also be used as a trust anchor.

Given the currently defined flags, in its text format, the flags field is represented as an unsigned decimal integer with the possible values of 0, 256 and 257. A value of 256 indicates that the DNSKEY record holds the ZSK and a value of 257 indicates that it contains the KSK. In general, this field contains an odd number when the DNSKEY record holds the KSK.
• Protocol: This always has a value of 3, for DNSSEC.
• Algorithm: Identifies the public key's cryptographic algorithm. The available types are:
  • 1 = RSA/MD5
  • 2 = Diffie-Hellman (This is not supported by BIND and Infoblox appliances.)
  • 3 = DSA
  • 4 = Reserved
  • 5 = RSA/SHA1
  • 6 = DSA/SHA1/NSEC3
  • 7 = RSA/SHA1/NSEC3
  • 8 = RSA/SHA-256
  • 10 = RSA/SHA-512
• Public Key: The public key encoded in Base64.

RRSIG Resource Records

A signed zone has multiple RRsets, one for each record type and owner name. (The owner is the domain name of the RRset.) When an authoritative name server uses the private key of the ZSK pair to sign each RRset in a zone, the digital signature on each RRset is stored in an RRSIG record. Therefore, a signed zone contains an RRSIG record for each RRset.

Following is an example of an RRSIG record:

```
<table>
<thead>
<tr>
<th>Owner Name</th>
<th>TTL</th>
<th>Class</th>
<th>RR Type</th>
<th>Type Covered</th>
<th>Algorithm</th>
<th>Number of Labels</th>
<th>Signature Name</th>
<th>Key Tag</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>corpxyz.com</td>
<td>86400</td>
<td>IN</td>
<td>RRSIG</td>
<td>A</td>
<td>5</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

The first four fields specify the owner name, TTL, class, and RR type. The succeeding fields are:

• Type Covered: The RR type covered by the RRSIG record. The RRSIG record in the example covers the A records for corpxyz.com.
• Algorithm: The cryptographic algorithm that was used to create the signature. It uses the same algorithm types as the DNSKEY record indicated in the Key Tag field.
• Number of Labels: Indicates the number of labels in the owner name of the signed records. There are two labels in the example, corpxyz and com.
• RRset TTL: The TTL value of the RRset covered by the RRSIG record.
• Expiration Time: The signature expiration time in UTC format.
• Inception Time: The signature inception time in UTC format.
• Key Tag: The key tag value of the DNSKEY RR that validates the signature.
• Signature Name: The zone name of the RRset.
• Public Key: The Base64 encoding of the signature.

NSEC/NSEC3 Resource Records

When a name server receives a request for a domain name that does not exist in a zone, the name server sends an authenticated negative response in the form of an NSEC or NSEC3 RR. NSEC and NSEC3 records contain the next secure domain name in a zone and list the RR types present at the NSEC or NSEC3 RR's owner name. The difference between an NSEC and NSEC3 RR is that the owner name in an NSEC3 RR is a cryptographic hash of the original owner name prepended to the name of the zone. NSEC3 RRs protect against zone enumeration.

Following is an example of an NSEC record:
The first four fields specify the owner name, TTL, class and RR type. The succeeding fields are:

- **Next Owner Name**: In the canonical order of the zone, the next owner name that has authoritative data or that contains a delegation point NS record.
- **RRsets**: The RRsets that exist at the owner name of the NSEC record, which are NS, SOA, RRSIG, NSEC, and DNSKEY in the example.

Following is an example of an NSEC3 RR:

![Diagram of NSEC3 RR]

The first field contains the hashed owner name. It is followed by the TTL, class and RR type. The fields after the RR type are:

- **Algorithm**: The hash algorithm that was used. The currently supported algorithm is SHA-1, which is represented by a value of 1.
- **Flags Field**: Contains 8 one-bit flags, of which only one flag, the Opt-Out flag, is defined by RFC 5155. The Opt-Out flag indicates whether the NSEC3 record covers unsigned delegations.
- **Iterations**: The number of times the hash function was performed.
- **Salt Field**: A series of case-insensitive hexadecimal digits. It is appended to the original owner name as protection against pre-calculated dictionary attacks.
- **Next Owner Name**: Displays the next hashed owner name.
- **RRsets**: The RR types that are at the owner name.

**NSEC3PARAM Resource Records**

An authoritative DNS server uses NSEC3PARAM RRs to determine which NSEC3 records it includes in its negative responses. An NSEC3PARAM RR contains the parameters that an authoritative server needs to calculate hashed owner names. As stated in RFC 5155, the presence of an NSEC3PARAM RR at a zone apex indicates that the specified parameters may be used by authoritative servers to choose an appropriate set of NSEC3 RRs for negative responses.

Following is an example of an NSEC3PARAM record:

![Diagram of NSEC3PARAM RR]

The first four fields specify the owner name, TTL, class and RR type. The succeeding fields are:

- **Algorithm**: The hash algorithm that was used. The currently supported algorithm is SHA-1, which is represented by a value of 1.
• Flags Field: Contains 8 one-bit flags, of which only one flag, the Opt-Out flag, is defined by RFC 5155. The Opt-Out flag indicates whether the NSEC3 record covers unsigned delegations.
• Iterations: The number of times the hash function was performed. The number of NSEC3 iterations is set to 10.
• Salt Field: A series of case-insensitive hexadecimal digits. It is appended to the original owner name as protection against pre-calculated dictionary attacks. New salt value is generated when the ZSK rolls over, for which the user can control the period. For random salt, the selected length is between one and 15 octets.

**DS Resource Records**

A DS RR contains a hash of a child zone's KSK and can be used as a trust anchor in some security-aware resolvers and to create a secure delegation point for a signed subzone in DNS servers. As illustrated in 4817290, the DS RR in the parent zone corpxyz.com contains a hash of the KSK of the child zone sales.corpxyz.com, which in turn has a DS record that contains a hash of the KSK of its child zone, nw.sales.corpxyz.com.

**Figure 22.1**

The first four fields specify the owner name, TTL, class and RR type. The succeeding fields are as follows:

• Key Tag: The key tag value that is used to determine which key to use to verify signatures.
• Algorithm: Identifies the algorithm of the DNSKEY RR to which this DS RR refers. It uses the same algorithm values and types as the corresponding DNSKEY RR.
• Digest Type: Identifies the algorithm used to construct the digest. The supported algorithms are:
  • 1 = SHA-1
  • 2 = SHA-256
• Digest: If SHA-1 is the digest type, this field contains a 20 octet digest. If SHA-256 is the digest type, this field contains a 32 octet digest.

**Configuring DNSSEC on a Grid**

You can configure the name servers in a Grid to support DNSSEC. You can configure the Grid Master as the primary server for a signed zone and the Grid members as secondary servers. (For more information, see Configuring Grid Members to Support DNSSEC as Secondary Servers.) Note that only the Grid Master can serve as the primary server for a signed zone.

You can enable the Grid Master to sign zones and manage the DNSSEC keys, or you can configure the Grid Master as a client to a third-party, network-attached Hardware Security Module (HSM) that performs the key generation, zone signing, and key safekeeping. You must use either the Grid Master or HSM for zone signing and key management; you cannot use both. Note that each method may have different performance implications, depending on the hardware platform, number of zones and other factors. For information about using HSMs, see About HSM Signing.

Any authoritative forward-mapping or reverse-mapping zone can be signed according to the following criteria:

• The zone does not contain any bulk host records.
• DNSSEC is enabled on the Grid Master.
• The primary server of the zone must be a Grid member. If the zone is assigned to an NS group, the primary server in the group must be a
Grid member that has DNSSEC enabled.

Note that you can use DNS views to separate internal and external zone data, to manage your zones more efficiently and reduce the size of the zones that require signing. For information about DNS views, see Using Infoblox DNS Views.

Grid Master as Primary Server

When you sign a zone whose primary server is a Grid member, that member becomes a secondary server and the Grid Master becomes the hidden primary server. If the zone is assigned to an NS group, the Grid Master removes the association with the NS group. The previous primary server becomes a secondary server for the zone.

If a Master Candidate is promoted to Grid Master and the previous Grid Master was the primary server for signed zones, the new Grid Master becomes the hidden primary server for all signed zones. The previous Grid Master, which was the primary server for the zone, becomes a secondary server for the zone.

As the primary server, the Grid Master sends zone data to the secondary servers through zone transfers; or, if the secondary servers are Grid members, the Grid Master transfers data to all Grid members through the database replication process, by default. The Grid Master transfers all records in that zone, including all NSEC/NSEC3, RRSIG, DNSKEY and DS records with owner names that belong to that zone. The RRSIG RRs are included in zone transfers of the zone in which they are authoritative data. The Grid Master also performs incremental zone transfers to secondary servers as a result of incremental zone signings.

In addition, the Grid Master automatically performs an incremental signing of the zone data sets when their contents change. Incremental signing refers to signing just those parts of a zone that change when RRs are added, modified, or deleted. The Grid Master uses the private key of the ZSK when it incrementally signs a zone. In addition, the Grid Master adds, modifies or deletes the corresponding RRSIG records and the appropriate NSEC/NSEC3 records.

For example, 4820062 shows a Grid Master as the primary server of a signed zone and its Grid members as secondary servers. The Grid Master, ns1.corpxyz.com, is the hidden primary DNS server for the corpxyz.com zone. As the hidden primary name server for corpxyz.com, the Grid Master does not respond to queries from other name servers. Instead, it provides data to its secondary servers, ns2.corpxyz.com and ns3.corpxyz.com, which use this data to respond to DNS queries. Because the secondary servers are Grid members, they receive zone data from the Grid Master through the Grid database replication process.

The name server ns1.corp200.com is a recursive name server. It has configured the DNSKEY of the corpxyz.com zone as a trust anchor. Therefore, it is able to validate the data it receives when it sends a query for the corpxyz.com zone.

Figure 22.2

Following are the tasks to configure the Grid Master to sign zones:

1. Create the zones. For information, see Configuring Authoritative Zones.
   - Specify the Grid Master as the primary server.

2. Enable DNSSEC, as described in Enabling DNSSEC.

3. Optionally, change the default DNSSEC settings. For information, see Setting DNSSEC Parameters.

4. Sign the zone. The appliance automatically generates the DNSSEC RRs when you sign a zone. For information, see Signing a Zone.
Enabling DNSSEC

You can enable DNSSEC on a Grid, individual members, and DNS views. Because only Grid Masters can serve as primary servers for signed zones, you must enable DNSSEC on the Grid Master before you can sign zones. You must also enable DNSSEC on any Grid member that serves as a secondary server for signed zones.

When you enable DNSSEC on a Grid, you can set certain parameters that control the DNSSEC RRs, as described in Setting DNSSEC Parameters.

When you enable DNSSEC on a Grid member or DNS view, you can set parameters that affect its operations as a secondary server, as described in Configuring Grid Members to Support DNSSEC as Secondary Servers.

To enable DNSSEC on a Grid, member or DNS view:

1. **Grid:** From the Data Management tab, select the DNS tab. Expand the Toolbar and click Grid DNS Properties.
   - **Member:** From the Data Management tab, select the Members tab -> member check box and click the Edit icon.
   - **DNS View:** From the Data Management tab, select the Zones tab -> dns_view check box and click the Edit icon.

2. In the editor, click **Toggle Expert Mode**. When the additional tabs appear, click **DNSSEC**.

3. In the DNSSEC tab, select **Enable DNSSEC**.

   **Note:** When you disable EDNS0, all outgoing DNSSEC queries to zones within trusted anchors will fail even if DNSSEC validation is enabled. This is due to the restriction of the UDP packet length when you disable EDNS0. For information about EDNS0, see Using Extension Mechanisms for DNS (EDNS0).

4. Save the configuration and click **Restart** if it appears at the top of the screen.

Setting DNSSEC Parameters

The Grid Master uses certain default parameters when it signs a zone and generates the DNSSEC RRs. You can change these defaults for the entire Grid and for individual zones, in case you want to use different parameters for certain zones. The following sections describe the different parameters that you can set:

- 4820067
- 4820067
- 4820067

For information on setting these parameters, see 4820067.

About the DNSKEY Algorithm

You can add multiple cryptographic algorithms that the Grid Master uses when it generates the KSK and ZSK. You can also add multiple algorithms at the Grid level and override them at the zone level. By default, the appliance uses RSA/SHA1 for both KSK and ZSK. You can add DSA, RSA/MD5, RSA/SHA1, RSA/SHA-256, or RSA/SHA-512 algorithms. However, you cannot add RSA/MD5 if the zone is signed with NSEC3 records. Note that a zone can contain either NSEC or NSEC3 records, but not both. You can add same or different set of algorithms with possibly different key sizes for both KSK and ZSK.

You can assign the DNSKey algorithm for HSMs. Thales HSMs don't support DSA. All other parameters are not used by HSMs.

About Key Rollovers

To reduce the probability of their being compromised, ZSKs and KSKs must be periodically changed. The time within which a key pair is effective is its rollover period. The rollover period starts as soon as a zone is signed. After a rollover period starts, you cannot interrupt or restart it unless you unsign the zone. During the key rollover, all the algorithms are rolled over at the same time and the rollover is performed on a per-zone basis.

Zone-Signing Key Rollover

You can configure automatic ZSK rollovers on the Grid Master, using the double signature rollover method or the pre-publish method. For more information, see 4820067. The appliance initiates the ZSK rollover of signed zones when they are due. You can also perform a manual rollover of ZSKs. For more information, see Rolling Zone-Signing Keys.

The double signature method provides a grace period, which is half of the rollover period. The default ZSK rollover period is 30 days; thus the default grace period is 15 days.

At the end of a rollover period of a ZSK, the Grid Master generates a new ZSK key pair. It signs the zone with the private key of the new ZSK key pair, and consequently generates new RRSIG RRs with the new signatures. However, the Grid Master also retains the old ZSK key pair and RRSIG RRs. Thus during the grace period, the data in the zone is signed by the private keys of both the old and new ZSKs. Their corresponding public keys (stored in DNSSEC RRs) can be used to verify both the old and new RRSIGs.

The grace period also allows the data that exists in remote caches to expire and during this time, the updated zone data can be propagated to all authoritative name servers. The Grid Master removes the old ZSK and its RRSIGs when the rollover grace period elapses. When a scheduled DNSSEC operation exists for a zone, the appliance does not lock it against other administrative changes and the administrator can still operate on
a given zone even if there is a pending DNSSEC operation scheduled for it. The appliance sets pre-publish method described in RFC 4641 as the default zone-signing key rollover method for NIOS 6.11.0 or later releases. In the pre-publish rollover method, the new key is published in the keyset before the actual rollover. After the key propagates to all client caches, Grid Master removes the old signatures and creates new signatures with the new keys. The pre-publish rollover method uses the current key to sign the zone.

**Key-Signing Key Rollover**

You can configure automatic KSK rollovers on the Grid Master or perform a manual KSK rollover. The default KSK rollover period is one year. The Grid Master also uses the double signature rollover method described in RFC 4641 for KSK rollovers. To configure automatic KSK rollovers, see Configuring Automatic KSK Rollovers and Notifications. For information about performing a manual KSK rollover, see Rolling Key-Signing Keys.

When the KSK rollover is overdue or is due within seven days, the Grid Master displays a warning when admins log in. In addition, you can also check which KSKs are due for a rollover as described in Checking Key-Signing Keys.

When a user initiates a KSK rollover, the Grid Master sets the grace period to half the KSK rollover period. It generates a new KSK, and signs the DNSKEY records with the new KSK. Thus during the grace period, the DNSKEY records are signed by the private keys of both the old and new KSKs. Both the old and the new KSKs can be used to validate the zone. The grace period allows the old keys in remote caches to expire. In addition, the admin should also export the new KSK and send it to the recursive name servers that use the KSK as trust anchors. If the KSK rollover is for a child zone and the primary server of the parent zone is a Grid member, the Grid Master also inserts a DS record in the parent zone for the new DNSKEY in the child zone. If the primary server of the parent zone is external to the Grid, the admin must export either the DS record or the new KSK to the admin of the parent zone. For information about exporting a KSK, see Exporting Trust Anchors.

The Grid Master then removes the old KSK and its RRSIG records when the grace period for the KSK rollover ends.

**About Key Rollovers and DNS TTLS**

Note that the KSK and ZSK rollover intervals affect TTLS used by RRs in signed zones.

A grace period is half of the key rollover interval. For example, if the KSK rollover interval is 1 year (365 days), then the grace period is 182.5 days; if the ZSK rollover interval is 30 days, then the grace period is 15 days.

The DNSKEY RRset in the zone is assigned a TTL, which is half of the signature validity interval. The default signature validity interval is set to 4 days, so DNSKEY RRset TTL is set to 2 days (172800 seconds). All other RRs in the signed zone is limited to a “zone maximum TTL,” which is the grace period of the ZSK. In the example, this is also 15 days. When the zone is initially signed, if the TTL of an RR exceeds the zone maximum TTL, the Grid Master reduces the TTL to the zone maximum TTL. Additionally, the TTL settings for the signed zone are set to override; the values are inherited from the Grid DNS properties at that time, and the default TTL setting is reduced to the zone maximum TTL if the Grid property exceeds it. If the zone is later unsigned, the zone DNS properties remain at their overridden settings.

**RRSIG Signatures**

As shown in the sample RRSIG record in RRSIG Resource Records, the signatures have an inception and an expiration time. The default validity period of signatures in RRSIG records on the Grid Master is four days. You can change this default, as long as it is not less than one day or more than 3660 days. The Grid Master automatically renews signatures before their expiration date.

**Configuring DNSSEC Parameters**

The following are the guidelines for choosing the DNSSEC parameters:

- RSA/SHA1 is the most widely used cryptographic algorithm for generating KSK and ZSK. However, it is recommended to use RSA/SHA-256 and RSA/SHA-512 for better interoperability.
- The usage of DSA cryptographic algorithm is optional. As stated in RFC 6944, it may not be supported by many systems.
- It is not recommended to use RSA/MD5 cryptographic algorithm as it is not very secure. As stated in RFC 6944, there are known defects in MD5.
- The key size of KSK algorithm is recommended to be equal to or greater than the key size of ZSK algorithm.

To set parameters at the Grid or zone level:

1. **Grid:** From the Data Management tab, select the DNS tab. Expand the Toolbar and click Grid DNS Properties. **Zone:** From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and click the Edit icon. Click Override to override the parameters.
2. **Standalone appliance:** From the Data Management tab, select the DNS tab. Expand the Toolbar and click System DNS Properties.
3. When the additional tabs appear, click DNSSEC.
4. In the DNSSEC tab, click the Basic tab and complete the following:
   - **Resource Record Type for Nonexistent Proof:** Select the resource record type (NSEC or NSEC3) you want to use for handling non-existent names in DNS. The default is NSEC3. The algorithms used by the KSK and ZSK can generate the same type of NSEC record. Note that a zone cannot contain both NSEC and NSEC3 resource records.
- **Key-signing Key**: Click the Add icon to add the cryptographic algorithm that the Grid Master or HSM uses when it generates the KSK. You can add multiple algorithms, but you cannot add the same algorithm more than once. Grid Manager adds a row to the table each time you click the Add icon. Select the row and the algorithm from the drop-down list and enter the key size for the algorithm. The default is `RSA/SHA1` with the key size `2048`.

  Following are the valid values for each algorithm:

  - **DSA**: The minimum is 512 bits and the maximum is 1024 bits, which is also the default. The key length must be a multiple of 64. Note that Thales HSMs do not support DSA.
  - **RSA/MD5**: The minimum is 512 bits, the maximum is 4096 bits, and the default is 2048 bits. You can configure this for NSEC only.
  - **RSA/SHA1**: The minimum is 512 bits, the maximum is 4096 bits, and the default is 2048 bits. **RSA/SHA-256**: The minimum is 512 bits, the maximum is 4096 bits, and the default is 2048 bits. **RSA/SHA-512**: The minimum is 1024 bits, the maximum is 4096 bits, and the default is 2048 bits.

- You can delete an algorithm by selecting it and clicking the Delete icon.

- **Key-signing Key Rollover Interval**: You can specify the key signing key rollover interval for all the algorithms. The minimum value is one day and the maximum is the time remaining to January 2038. The default is one year.

- **Zone-signing Key**: Click the Add icon to add the cryptographic algorithm that the Grid Master or HSM uses when it generates the ZSK. You can add multiple algorithms, but you cannot add the same algorithm more than once. Grid Manager adds a row to the table each time you click the Add icon. Select the row and the algorithm from the drop-down list and enter the key size for the algorithm. The default is `RSA/SHA1` with the key size `1024`.

  Following are the valid values for each algorithm:

  - **DSA**: The key length must be a multiple of 64. The minimum is 512 bits and the maximum is 1024 bits. The default is 1024 bits. Note that Thales HSMs do not support DSA.
  - **RSA/MD5**: The minimum is 512 bits, the maximum is 4096 bits, and the default is 2048 bits. You can configure this for NSEC only.
  - **RSA/SHA1**: The minimum is 512 bits, the maximum is 4096 bits, and the default is 1024 bits.
  - **RSA/SHA-256**: The minimum is 512 bits, the maximum is 4096 bits, and the default is 1024 bits.
  - **RSA/SHA-512**: The minimum is 1024 bits, the maximum is 4096 bits, and the default is 1024 bits.

- You can delete an algorithm by selecting it and clicking the Delete icon.

- **Zone-signing Key Rollover Interval**: You can specify the zone signing key rollover interval for all the algorithms. The minimum value is one day and the maximum is the time remaining to January 2038. The default is 30 days.

- **Signature Validity**: Specify the signature validity period for RRSIG RRs. The minimum is one day and the maximum is 3660 days. The default signature validity interval is four days.

- **Zone-signing Key rollover method**: You can use either of these methods to sign all the RRsets in a zone:
  - **Pre-publish**: Select this if you want to use the pre-publish signature scheme to sign all the RRsets in a zone while performing the ZSK rollover. When you select this option, the record sets are signed using a single key. The appliance sets this option as the default zone-signing key method for NIOS 6.11.0 and later releases.
  - **Double Sign**: Select this if you want to use the double signature scheme to sign all the RRsets in a zone while performing the ZSK rollover. The non-DNSKEY RRset are signed twice, which increases the size of the zone files.

  **Note**: You can select the **Zone-signing Key rollover method** only after you enable DNSSEC.

5. Save the configuration and click **Restart** if it appears at the top of the screen.

When you modify the algorithms for a signed zone, you can apply the algorithm changes to the zone, as described in [4820067](https://example.com) or you can unsign the zone and sign it again. For an unsigned zone however, you can apply the algorithm changes by signing the zone. For information about signing a zone, see [Signing a Zone](https://example.com).

When you re-sign a zone after adding an algorithm, the DNSKEY key pairs of the old algorithms are rolled over and all the old RRSIG records are removed. The zone is re-signed with the new DNSKEY key pairs. When you re-sign a zone after removing an algorithm, the DNSKEY key pairs of the remaining algorithms are rolled over and the DNSKEY RRset of the removed algorithm is removed. All old RRSIG records are removed and the zone is re-signed with the new DNSKEY key pairs.

**Note**: If you add or remove a KSK algorithm from a zone, you must update the DS RRsets at the parent zone when the parent zone is managed by a non-Infoblox DNS server or an Infoblox server that is part of a different Grid. For information, see [Importing a Keyset](https://example.com).

### Applying the Algorithm Changes

You can apply the algorithm changes to a zone whenever the KSK or ZSK algorithms are modified. You can apply the algorithm changes only to a signed zone.

To apply the algorithm changes to a signed zone:

1. From the **Data Management** tab, select the **DNS** tab.
2. Expand the Toolbar and click **DNSSEC -> Apply Algorithm Changes**.
3. In the **Apply Algorithm Changes** dialog box, click the **Add** icon to select a zone. When there are multiple zones, Grid Manager displays the **Zone Selector** dialog box. The appliance displays signed zones only. Select a zone. To add multiple zones, click the **Add** icon and select a zone.

   To remove a zone from the list, select the check box adjacent to the respective zone and click the **Delete** icon.

   You can click the **Schedule** icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, either select **Now** or select **Later** and enter a date, time, and time zone.

4. After you have selected the zones, click **Apply Algorithm Changes**.
5. When the confirmation dialog appears, click Yes.

Deleting the DNSSEC Keys Associated with a Zone

You can view the status of KSKs and ZSKs or delete the existing keys. Note that you can only delete keys that are either published or rolled over. You cannot delete keys that are active.

To delete keys:

1. From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and click the Edit icon.
2. In the Authoritative Zone editor, click the DNSSEC tab, and the following are displayed in the Advanced tab:
   - **Key ID**: The appliance generates a separate ID for each key. Select the check box adjacent to the Key ID. To delete an KSK, select the check box in the Key-signing Keys table. Select the check box in the Zone-signing Keys table to delete an ZSK.
   - **Status**: The Status column displays the status of the respective key. It can be one of the following: Active, Published, or Rolled.
   - **Public Key**: This column displays the public key that is associated with the respective KSK or ZSK.
   - **Algorithm**: This column displays the algorithm that is associated with the respective KSK or ZSK.
   - **Time until next event**: This column displays the time that is left to perform the next action for a key that is associated with the respective ZSK. This column help you decide whether to roll over manually or wait for a zone to resign automatically. The time is displayed in months, days, hours format. For example, 2m 3d 13 h implies time left to perform the next action is 2 months, 3 days and 13 hours.
     - **Active Key**: Indicates the time when the active key is rolled and zone is signed with the published key.
     - **Published Key**: Indicates the time when the published key is used to resign a zone.
     - **Rolled Key**: Indicates the time when a rolled key is deleted. Rolled keys are stored for quite a long period of time and are not used. You can manually cleanup the rolled keys.
3. Click the Delete icon.

Signing a Zone

When it signs a zone, the Grid Master generates new DNSKEY key pairs. As shown in 4820072, it uses the private key of the ZSK to sign the authoritative RRsets in the zone, and stores the corresponding public key in a DNSKEY record. It then uses the private key of the KSK to sign the DNSKEY records and stores the corresponding public key in another DNSKEY record. It stores the private keys in the Grid database and stores the public keys in the DNSKEY records in the database.

![Zone Signing Process](image)

The Grid Master also does the following:

- It inserts NSEC or NSEC3 records. The use of NSEC or NSEC3 records depends on the NSEC type you selected for the Grid or the zone. When you select NSEC3, the Grid Master uses NSEC3 records in signed zones.
- It increments the SOA serial number and notifies the secondary servers that there is a change to its zone data. When the secondary servers check the serial number and see that it has been incremented, the secondary servers request a zone transfer.
- If the TTL of an RR in the zone exceeds the ZSK grace period, the Grid Master reduces the TTL to the ZSK grace period. (For
information about the grace period, see About Key Rollovers.) Setting a TTL value that exceeds half of the rollover period is not allowed.
- If the KSK rollover period is less than the ZSK rollover period, the Grid Master sets the TTL of the DNSKEY RR to the KSK rollover period.
- The appliance sets the Grid Master as the primary server for zones, enables DNSSEC on the Grid Master, and starts DNS service on the Grid Master.

When it signs a subzone, the Grid Master automatically inserts DS records for parent zones that are hosted by Grid members. The appliance allows you to sign a single zone or multiple zones simultaneously. For example, if you have multiple zones that are due for rollover at the same time, you can select all such zones and sign them at once. Note that each operation is independent of the other. For example, if you want to sign five zones at the same time, and if one of the zones fails during this time, NIOS signs the remaining four zones. Note that the selected zones must have an associated primary server. The appliance displays an error message if the zone does not have a primary server. When the sign operation fails, the appliance displays the zone names, associated DNS views, and the error message indicating the reason for failure.

To sign a zone:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Sign Zones.
3. In the Sign Zones dialog box, the displayed zone name can either be the last selected zone or the zone from which you are signing. If no zone name is displayed or if you want to select a different zone, click the Add icon. The appliance displays unsigned zones only. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Select a zone. To add multiple zones, click the Add icon and select a zone.
   You can click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, either select Now or select Later and enter a date, time, and time zone. For information, see Scheduling Tasks.
4. After you have selected the zones, click Sign Zones.
5. When the confirmation dialog displays, click Yes.

When you sign multiple zones, the appliance displays generic error messages for the following cases:
- The value to which the resource record TTL is reduced is not displayed.
- The appliance displays a message about name server group disassociation if at least one zone is associated with a name server group. It will not list the affected zones.
- When you sign a zone or multiple zones, the appliance displays a warning message indicating that the operation might take a longer time.
- The appliance displays an error message if the number of characters in the zone name, which you want to sign, exceeds 180 characters. You can sign a zone only when the name of the zone is less than 180 characters in size.

To remove a zone from the list, select the check box adjacent to the respective zone and click the Delete icon. To view the records of the signed zone, from the Data Management tab, select the DNS tab -> Zones tab -> zone. Expand the Records section to list the RRs of the zone, as shown in 4820072.

Figure 22.4

Managing Signed Zones
After you sign a zone, you can do the following:
- You can add a DS RR at the delegation point for a signed subzone when the subzone is hosted on a non-Infoblox DNS server or an
Infoblox server that is part of a different Grid. For information, see 4820072.

- Trust anchors can be specified as DNSKEY RRs, DS RRs, and as a BIND trusted-keys statement. You can export any of these as trust anchors. For information, see 4820072.
- You must change the KSK periodically, to ensure its security. For information, see 4820072 and 4820072.
- You can initiate ZSK rollovers manually. For information, see 4820072.
- If, for any reason, the security of the keys are compromised, you can delete a key and perform a manual rollover. For information, see 4820072.
  Note that when you re-sign a zone, the Grid Master generates new ZSK and KSK pairs. You must send the new DNSKEY of the KSK to resolvers that use it as a trust anchor and generate new DS records and send them to the parent zones.
- You can move a signed zone to the Recycle Bin, from where you can delete it permanently or restore it. For information, see 4820072.

In addition, signed zones can accept dynamic DNS updates. For information about configuring zones to accept dynamic DNS updates, see Configuring DNS Servers for DDNS.

### Importing a Keyset

A keyset is a DS RRset, or a DNSKEY RRset which is used as input to generate the DS RRset. To import a keyset:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Import Keyset.
3. In the Import Keyset dialog box, the displayed zone name can either be the last selected zone or the zone from which you are importing the keyset. If no zone name is displayed or if you want to select a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box from which you can select a zone.
4. Paste the KSK or DS record being imported. It must be a KSK or DS record, and must belong to an immediate subzone of the zone to which the record is being imported.
5. Click Import.

If you imported a DNSKEY RRset, the Grid Master uses the SHA-1 algorithm to generate the DS RRset, which it adds to the parent zone. If you imported a DS RRset, the Grid Master adds it to the parent zone. The Grid Master incrementally signs the DS RRset.

### Exporting Trust Anchors

A trust anchor is a DNSSEC public key which is used by security-aware resolvers as the starting point for establishing authentication chains. A trust anchor can be specified as a DNSKEY RR or a DS RR, which contains the hash of a DNSKEY RR and can also be used to create a secure delegation point for a signed subzone in DNS servers.

In BIND, trust anchors are configured using the trusted-keys directive. A trusted key is a DNSKEY RR without the TTL, class and RR type. You can export the trust anchors for the selected zone in a format that can be used in a BIND trusted-keys directive. Exporting trust anchors supports multiple algorithms, which means you can export all the algorithms in a key.

To export trust anchors:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Export Trust Anchors.
3. In the Export Trust Anchors dialog box, do the following:
   - The displayed zone name can either be the last selected zone or the zone from which you are exporting trust anchors. If no zone name is displayed or if you want to select a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box from which you can select one.
   - Select one of the following: DNSKEY records, DS records, or BIND trusted-keys statement.
4. Click Export.
5. Specify the location of the exported file and click OK.

If you exported DS records, the exported file contains DS records that use the SHA-1 and SHA-256 algorithms.

### Checking Key-Signing Keys

To check which key-signing keys are overdue for a rollover or are due to roll over within a week:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Check KSK Rollover Due.
3. The KSK Rollover Due dialog box lists the key-signing keys that are due to rollover. It includes the domain name of the zone, DNS view (if there are multiple DNS views), and the number of days until the rollover.
4. You can click the Schedule icon at the top of the wizard to schedule a KSK rollover for one or more zones at a given date and time. In the Schedule Change panel, either select Now or select Later and enter a date, time, and time zone. For information, see Scheduling Tasks.
5. Click Close.

### Rolling Key-Signing Keys

You can initiate a rollover before or after a rollover period, or when you need to replace the KSK for security reasons. You can initiate a KSK
To roll over key-signing keys:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Roll Over Key-Signing Key.
3. In the Roll Over Key-Signing Key dialog box, the displayed zone name can either be the last selected zone or the zone from which you are rolling over key-signing keys. If no zone name is displayed or if you want to select a different zone, click the Add icon. The appliance displays signed zones only. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. To add multiple zones, click the Add icon and select a zone.
   You can click the Schedule icon at the top of the wizard to schedule a KSK rollover for one or more zones at a given date and time. In the Schedule Change panel, either select Now or select Later and enter a date, time, and time zone. For information, see Scheduling Tasks. Note that you cannot schedule the KSK rollover on a recurring basis.
4. Click Roll Over.

You can export the new KSK and send it to the security-aware resolvers that use it as a trust anchor. To remove a zone from the list, select the check box adjacent to the respective zone and click the Delete icon.

Rolling Zone-Signing Keys

Only an administrator can initiate ZSK rollovers either before or after a rollover period, or when you want to replace the ZSK for security reasons. You can initiate a ZSK rollover several times simultaneously, but note that the number of keys will increase each time you perform a rollover.

To roll over zone-signing keys:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Roll Over Zone-Signing Key.
3. In the Roll Over Zone-Signing Key dialog box, the displayed zone name can either be the last selected zone or the zone from which you are rolling over zone-signing keys. If no zone name is displayed or if you want to select a different zone, click the Add icon. The appliance displays unsigned zones only. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. To add multiple zones, click the Add icon and select a zone.
   You can click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, either select Now or select Later and enter a date, time, and time zone. For information, see Scheduling Tasks.
4. Click Roll Over.

To remove a zone from the list, select the check box adjacent to the respective zone and click the Delete icon. The appliance displays warning messages when the changes take effect on the first zone or when the rollover occurs. You cannot change the zone-signing key rollover method while the previous change is still in progress. The previous change will be completed only when the zone active key, which is active when the rollover method is changing, expires and is deleted.

Best Practices for Configuring Zone Signing Keys

Infoblox recommends that you use the pre-publish option for zone signing key method for the following reasons:

- The double-signature ZSK rollover doubles the number of signatures in your zone when a rollover is in progress. The size of the zone increases due to the duplicate signature records. This is not recommended if the size of your zones are large. When you select this option, the appliance creates a new set of signatures for all the resource records. This also increases the database usage.
- When you select to pre-publish key rollover, the rollover uses a single key to sign the records at a given time and it does not sign the zone data twice. The appliance publishes the new key in the keyset even before the actual rollover. This reduces the database usage.

Unsigning a Zone

When you unsign a zone, the Grid Master permanently removes all automatically generated DNSSEC records in the zone and parent zone. It does not remove any DS records associated with a child zone. You can unsign a single zone or multiple zones at the same time.

To unsign a zone:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Unsign Zones.
3. In the Unsign Zones dialog box, the displayed zone name can either be the last selected zone or the zone from which you are unsigning. If no zone name is displayed or if you want to select a different zone, click the Add icon. The appliance displays signed zones only. Select a zone. To add multiple zones, click the Add icon and select a zone.
   You can click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, either select Now and click Save or select Later and enter a date, time, and time zone. For information, see Scheduling Tasks.
4. After you have selected the zones, click Unsign Zones.
5. When the confirmation dialog displays, click Yes.

To remove a zone from the list, select the check box adjacent to the respective zone and click the Delete icon.
Deleting and Restoring Signed Zones

When you delete a signed zone, the Grid Master unsigns the zone before moving it to the Recycle Bin. Unsigning the zone effectively deletes all auto-generated DNSSEC RRs; only user-defined DS records are retained and moved to the Recycle Bin as well. The Grid Master also retains the ZSK and KSK in its database, until you permanently delete the zone from the Recycle Bin.

When you restore a signed zone, the Grid Master restores it and re-signs its data sets with the original keys, which are also restored. You can also restore the user-defined DS records. The rollover period of the ZSK and KSK starts when the zone is signed after it is restored. Note that when you restore a zone that contains rolled keys, either KSK or ZSK, the appliance removes all these rolled keys.

Note that when you restore a deleted zone from recycle bin on the NIOS server, which is created and signed on the Microsoft Server 2012, then all the DNSSEC records will be deleted, except for the DNSKEY records. The DNSKEY records will only be resynchronized. The DNSSEC records are read-only and cannot be regenerated using NIOS. You must recreate the zone manually on the Microsoft Server. When you recreate the zone on the Microsoft Server, new keys will be generated. The signed zone, which is restored, and the DNSSEC keys are synced to Microsoft Server. This zone will be seen as an unsigned zone on the Microsoft Server, as NIOS does not trigger the signing zone request for the corresponding zone. For such zones, the 'DNSSEC' label is not displayed and the value for 'Signed' column is 'No'.

To delete a signed zone:
1. From the Data Management tab, select the DNS tab -> Zones tab.
2. Click the check box of the zone you want to delete.
3. Click the Delete icon.
4. Click Yes to confirm the deletion.

To restore a signed zone:
1. In the Finder panel, expand Recycle Bin.
2. Select the zone you want to restore.
3. Click the Restore icon.

Configuring Automatic KSK Rollovers and Notifications

You can configure automatic KSK rollovers at the Grid level and override the settings at the zone level. You can also configure notifications for KSK rollovers. The appliance sends one notification, SNMP, or email, or both based on the selection, for each event. For example, if the KSK of two zones are rolled over in the same batch, the appliance sends two notifications, one for each zone. Note that the appliance sends these notifications only once, and they are not recurring. Apart from the notifications that you receive, Grid Manager also displays a banner when you log in to the Grid indicating that the KSK rollover is due within the next seven days. These notifications are not applicable to an ZSK; as the ZSK rollover is an automated process. The appliance generates numerous notifications.

To configure KSK rollover, complete the following:

1. Grid: From the Data Management tab, select the DNS tab. Expand the Toolbar and click Grid DNS Properties.
   Zone: From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and click the Edit icon. Click Override to override the values at the zone level.

   Standalone appliance: From the Data Management tab, select the DNS tab. Expand the Toolbar and click System DNS Properties.
2. Select the DNSsec tab and complete the following in the Basic tab:
   - KSK Notification Configuration: You can choose to receive notifications for KSK rollover events.
     - No Notifications: Select this if you do not want to receive any notifications for KSK rollover events.
     - Notifications for all KSK rollover events: Select this if you want to receive notifications for all KSK rollover events. The appliance sends notifications after the rollover.
     - Notifications only for KSK rollover events requiring manual DS update to parent zone: Select this if you want to receive notifications only for KSK rollover events that require manual DS updates to parent zone. This is selected by default.
     - Enable KSK Email Notification: Select this to receive email notifications about DNSSEC keys.
     - Enable KSK SNMP Notification: Select this to receive SNMP trap alerts about DNSSEC keys.
3. Enable automatic KSK rollover: This is selected by default. When you select this option, the appliance will automatically roll over KSKs when they are due. The appliance starts the rollover process at most six hours after the due date. The appliance logs the messages in the syslog.

Note: The appliance enables notifications and automatic KSK rollover by default for NIOS 6.11.0 and later releases. These are not available for earlier releases. Similar to automatic ZSK rollover, the appliance automatically restarts the DNS service after a KSK is rolled over.

4. Save the configuration.

Configuring NSEC3 Salt Length and Hashing Iterations

The salt is a random string, which is appended to the domain name before it gets hashed. The number of iterations indicates the number of additional times the hashing occurs. These serve as a protection against dictionary attacks. The appliance generates a new salt for initial signing and changes it every time a ZSK rollover occurs. Note that when you use a longer salt and higher number of iterations, DNS is more secure and the chances of dictionary attacks on NSEC3 are reduced.

You can choose the minimum and the maximum salt length at the Grid level and override them at the zone level. Note that the length of the salt has an impact on the size of the NSEC3 record, but it does not have an impact on the performance of the appliance.
When the number of iterations increases, the DNS client has to validate additional data and the cost of the DNS server to serve the zone increases. This might also reduce the performance of the system with regards to DNSSEC operations.

To define salt length and hashing iterations, complete the following:

1. **Grid:** From the Data Management tab, select the DNS tab. Expand the Toolbar and click Grid DNS Properties. From the Zone tab, select the Settings tab. Expand the Toolbar and click DNS Properties.

2. **Standalone appliance:** From the Data Management tab, select the DNS tab. Expand the Toolbar and click System DNS Properties.

To define salt length and hashing iterations, complete the following:

- **Zone-signing Key Settings**
  - **NSEC3 Salt Length:** Specify a minimum and a maximum length for NSEC3 salt. The minimum length is one octet and the maximum length is 255 octets. The appliance sets the following default values for minimum and maximum lengths respectively: one and 15 octets.
  - **Number of NSEC3 hashing iterations:** The appliance uses the default value, ten, for hashing iterations. The minimum value is ten and the maximum value depends on the smallest key size, as defined in RFC 5155 as follows:
    - 150 if the key size is equal or less than 1024 bits.
    - 500 if the key size is equal or less than 2048 bits.
    - 2,500 if the key size is equal or less than 4096 bits.

Note: The above fields are displayed only when you select NSEC3 record type.

**Deleting Server Keys**

The appliance retains the key until the expiration of the grace period. For example, if the validity period of a KSK is two years, you can delete the rolled key after publishing the DS record to the parent zone and waiting for a period greater than its TTL. The following rules are valid for KSK and ZSK signing using the double-signature scheme:

- You cannot delete an active key.
- When you delete a rolled key, the appliance displays a warning message indicating that it might break validation on clients.

The following rules are valid for ZSK signing using the pre-publish scheme:

- You cannot delete an active key.
- When you delete a pre-published key, the appliance generates a new pre-published key.
- You can delete a rolled key. The appliance deletes this key as it is no longer used.

When you use an HSM, the appliance does not delete the key from HSM. For more information, see *About HSM Signing*.

**Configuring Emergency KSK Rollover**

The appliance supports emergency rollover that can be used when the keys are compromised. In an emergency operation, you must delete the compromised key and the associated compromised data from the zone. The ability to perform emergency rollovers enable administrators to react quickly when a zone is compromised. To initiate an emergency rollover, you must first perform a manual rollover. For information about rolling over a KSK manually, see 4820072. After the rollover, you must delete the compromised key. For information about deleting the compromised key, see 4820072.

An emergency KSK rollover involves the following:

- The administrator of the compromised zone, which is hosted on the Infoblox appliance, must initiate the emergency KSK rollover and later export the corresponding DS record.
- The administrator of the parent zone, which is hosted on an external server, must import the DS record of the child zone. This is required to maintain the chain of trust.

During this emergency procedure, the chain of trust is temporarily broken. As stated in RFC 6781, the effect depends on the order of the operations:

- You must perform the KSK rollover first. The chain of trust is broken until the administrator of the parent zone replaces the DS record. In the meantime, the zone appears bogus to a validating client.
- You must remove the compromised DS record first. The chain of trust is broken until the NIOS administrator performs the KSK rollover, communicates the new DS record to the administrator of the parent zone who then adds it. In the meantime, the zone appears insecure to validating resolvers.

**Handling Error and Warning Messages for DNSSEC Operations**

Grid Manager consolidates warnings from one or more DNSSEC long running operations and displays them in a single dialog box. For more information about long running tasks, see *About Long Running Tasks*. When the long running operations are completed with warnings, the appliance displays the message using a yellow banner at the top of Grid Manager. Click *Show Warnings* to view the warnings that are generated by the server for DNSSEC operations. Click *Close* to close the warning dialog box.

The appliance also displays a warning icon in the Execution Status column of the Task Manager. For more information about the task manager, see *Viewing Tasks*. When you click the icon, the appliance displays a dialog box indicating that the task is complete with warnings. Click the sho
**w task details** hyperlink to view detailed information about the error or warning message. The appliance displays *Scheduled Task Details* wizard in which you can view the task details and error or warning messages, if any. For more information, see 4820072. The appliance clears the warning messages from the cache when you close the dialog box.

When a DNSSEC operation fails, NIOS saves the messages in the syslog. For more information about the syslog, see *Using a Syslog Server*.

### Viewing Scheduled Tasks

You can view the status of operations that are scheduled. The appliance also displays error or warning messages, if any. For example, if you schedule the *Sign Zones* operation for multiple zones, there is a possibility that some operations may fail, some may succeed with warnings, and some are completed successfully. You can also view the error or warning messages that are generated for certain affected zones. To view the status:

1. From the *Administration* tab, select the *Workflow* tab -> *Task Manager* tab.
2. Grid Manager displays the DNSSEC operations that are scheduled. To view the details you can either click the Action icon next to the task ID and select *View* from the menu or select the check box adjacent to the Action icon and then click *View* from the Toolbar.
3. The *General* tab of the *Scheduled Task Details* wizard displays the following details:
   - **Task ID**: The ID associated with the task. The appliance assigns an ID to a task in chronological order. By default, the appliance sorts tasks by **Task ID**.
   - **Action Type**: The operation the appliance performs in this task.
   - **Submitter**: The username of the admin who scheduled or submitted the task.
   - **Submitted Time**: The date, time, and time zone when the task was submitted.
   - **Ticket Number**: For an approval workflow, this number may be entered by the submitter to associate the task with a help desk ticket number or a reference number.
   - **Approver**: The username of the admin who has approved this task.
   - **Approver Comments**: Comments entered by the approver.
   - **Executed on Member**: The Grid member on which the task is executed.
   - **Execution Status**: The execution status of the task. Possible values are Completed, Failed, Pending, and Executing.
   - **Affected Objects**: The name of the object and object type.
4. The *Warnings/Errors* tab of the *Scheduled Task Details* wizard displays error or warning messages related to tasks. It also displays object execution details. This table is blank if there are no error messages or warnings. You can view the error message and the name of the zone with which the error or warning message is associated.
5. Click *Close* to close the dialog box.

### About HSM Signing

You can integrate a Grid with third-party, network-attached Hardware Security Modules (HSMs) for secure private key storage and generation, and zone-signing off-loading. Infoblox appliances support integration with either SafeNet HSMs or Thales HSMs. When using a network-attached HSM, you can provide tight physical access control, allowing only selected security personnel to physically access the HSM that stores the DNSSEC keys. When you enable this feature, the HSM performs DNSSEC zone signing, key generation, and key safe keeping. Note that if you migrate from using the Grid Master to HSMs, HSM signing starts at the next key rollover. Only a superuser can configure this feature. To configure HSM signing in a Grid, do the following:

1. Create the HSM group and add HSMs to the group. You can create either a SafeNet HSM group or a Thales HSM group. You can use only one group at a time. After you add the HSM group, the Add icon and Add button in the Toolbar are greyed out.
   - For information on adding a SafeNet HSM group, see Configuring a SafeNet HSM Device.
   - For information on adding a Thales HSM group, see Adding and Managing a Thales HSM Group.

   Note that if you delete an HSM or an HSM group, it is permanently deleted. It is not stored in the Recycle Bin.

2. Enable HSM signing. For information, see Enabling HSM Signing.

After you enable this feature, you can monitor the HSM group, as described in Monitoring the HSM Group. In addition, the Grid sends SNMP traps when zone signing succeeds or fails. For information about these traps, see Processing and Software Failure Traps.

Note that NIOS does not provide key life cycle management functions; these are handled by the HSM and must be configured via the HSM's administrative interface to adhere to corporate policies on key management. The keys (ZSK and KSK) used for DNSSEC are stored securely on the HSM and are not deleted by NIOS when the key is no longer required by the DNSSEC function. However, references to the keys are removed from the appliance.

### Configuring a SafeNet HSM Device


You can integrate a Grid with a SafeNet HSM group. The SafeNet HSM group can contain either SafeNet Luna SA 4, Luna SA 5, or Luna SA 6 devices in standalone or HA mode; the group cannot contain a mix of both models. You must first configure each HSM device, as described in Configuring a SafeNet HSM Device, and then create the group and add the devices to the group, as described in Adding a SafeNet HSM Group.

Configuring a SafeNet HSM Device

Do the following for each SafeNet HSM device that you are adding to the group:

1. On the Grid, generate a client certificate for the Grid Master and Grid Master Candidate. For information, see About Client Certificates.
2. On the SafeNet HSM, do the following:
   - Assign the Grid Master and Grid Master Candidate to a partition on the HSM to avoid any service interruptions, in case the Grid Master Candidate is promoted to Grid Master.
   - Upload the certificates of the Grid Master and Grid Master Candidate to the HSM and register the certificates in the HSM's list of clients. The certificates of the Grid Master and Grid Master Candidate are linked to their IP addresses. Therefore, if any of their IP addresses change, you must generate a new client certificate and register it with the HSM.
   - Note that if the HSM is configured and you replace an appliance that was a Grid Master or Grid Master Candidate and you backed up the database of the old appliance and restored it on the replacement appliance, the certificates remain intact. Therefore, you do not need to regenerate a new certificate for the replacement, as long as the IP address does not change.
   - If you are upgrading from a previous version of SafeNet HSM to a later version, such as from Luna SA5 to Luna SA6, you must complete the following before adding the new SA6 configuration to NIOS:
     - Remove the previous certificate registration from the HSM server and then re-register the Grid Master and Grid Master Candidate certificates.
     - Generate a new HSM certificate if you want to retain the current IP settings for the Grid Master.
   - Download the HSM certificate.

Note: Make sure that the common name used in the certificates is distinct when you configure HSM servers in HA mode.

For additional information, refer to your SafeNet HSM documentation.

Adding a SafeNet HSM Group

When you configure a SafeNet HSM group, add the SafeNet HSM devices to the group and upload their certificates to the Grid. You can add only one HSM group. To add a SafeNet HSM Group:

1. From the Grid tab, select the HSM Group tab.
2. Click the Add drop-down list and select HSM SafeNet Group.
3. In the Add HSM SafeNet Group wizard, complete the following and click Next:
   - Name: Enter a name for the HSM group.
   - Partition Password: Enter the partition password, and re-enter it in the Confirm Partition Password field.
   - Version: Select the SafeNet HSM version, which is either LUNA SA 4, LUNA SA 5, or LUNA SA 6.
   - Comment: You can enter additional information about the HSM.
4. Click the Add icon to add a SafeNet HSM device, and complete the following:
   - Name or IP Address: Enter the hostname or IP address of the HSM device.
   - Partition SN: Enter the partition serial number (PSN) of the HSM. The Partition ID field automatically displays the ID after the configuration is saved and the appliance has successfully connected to the device.
   - Disabled: Select this check box to disable use of this HSM.
   - Server Certificate: Upload the certificate of the SafeNet HSM.
5. Save the configuration.

After you add the HSM group, the Add icon and Add button in the Toolbar are greyed out. Note that if the HSM is configured in FIPS 140-2 compliant mode, certain key algorithms and key sizes are disallowed. Requests for those key algorithms or key sizes result in an error. The following algorithms are FIPS 140-2 compliant: DSA, DSA/NSEC3, RSA/SHA1, RSA/SHA1/NSEC3, RSA/SHA-256, and RSA/SHA-512. For additional information about selecting key algorithms, see About the DNSKEY Algorithm.

You can verify whether the Grid Master Candidate is properly registered with the HSM by navigating to the Grid -> Grid Manager -> Members page. It's Status icon is yellow if it is not registered with the HSM. If DNS service is enabled, you can also verify whether the Grid Master was able to contact the SafeNet HSMs by navigating to the Data Management > DNS > Members page. If the Grid Master status is yellow, check the status of the HSMs in the Grid > HSM Group page. (For more information, see Monitoring the HSM Group.) If the status is not green, check the configuration of the HSMs and restart the DNS service.

Adding and Managing a Thales HSM Group

On the Thales HSM, configure the Grid Master and Grid Master Candidate as HSM clients. Enroll the IP addresses of both the Grid Master and Grid Master Candidate to avoid any service interruptions, in case the Grid Master Candidate is promoted to Grid Master. If the Grid Master and Grid Master Candidates are HA pairs, you must enroll their VIPs.

Note: In the unlikely event that the Grid Master Candidate was registered with the Thales HSM after the Grid Master promotion, you must restart the DNS service on the newly promoted Grid Master.
In addition, you must also set up client cooperation to allow both the Grid Master and Grid Master Candidate access to the Remote File Server (RFS). Note that anytime you add a new Grid Master Candidate, you must enroll its IP address and set up a client cooperation to allow it access to the RFS. For more information on these procedures, refer to your HSM documentation.

Note that DSA cannot be used as the DNSSEC cryptographic algorithm for Thales HSMs. Therefore, migrating to Thales HSMs is not allowed if the Grid Master uses DSA as the DNSSEC cryptographic algorithm.

You can create one Thales HSM group in the Grid, and then add HSMs to the group. The appliance tries to connect to each of the HSMs in the order that they are listed.

To add a Thales HSM group:

1. From the **Grid** tab, select the **HSM Group** tab and click the Add icon.
2. In the **Add HSM Group** wizard complete the following, and then click **Next**:
   - **Name**: Enter a name for the HSM group.
   - **Protection**: Select the level of protection that the HSM group uses for the DNSSEC key data.
     - **Module**: Select this if the HSM group uses a module-protected key. You do not have to enter a password phrase for this type of key.
     - **Softcard**: Select this if the HSM group uses a softcard-protected key. You must then specify the card name and password.
   - **Card Name**: Enter a name for the softcard.
   - **Password Phrase**: Enter the password and re-enter it in the **Confirm Password Phrase** field.
   - **RFS IP Address**: Enter the remote file server (RFS) IP address. Note that you must ensure that you enter a valid RFS IP address for the Security World. Validation is limited to IP address checking. Infoblox recommends that you use **Test HSM Group** to check the HSM group configuration before proceeding.
   - **RFS Port**: Specify the port of the RFS.
   - **Comment**: Optionally, enter additional information about the group.
3. To add modules to the group, click the Add icon and complete the following:
   - **Remote IP**: Enter the IP address of the HSM.
   - **Remote Port**: Specify the destination port on the HSM. The firewall must be configured to allow connection to this port.
   - **Disabled**: Select this check box to disable use of this HSM.
   - **Keyhash**: Enter the keyhash, which is displayed on the console of the HSM. It can be obtained through an out of band mechanism from the HSM administrator. Note that the appliance validates the keyhash. If the entry is correct, the appliance displays the Electronic Serial Number (ESN) of the HSM when the editor is next launched. If the keyhash is incorrect, the appliance does not connect to the HSM.
   - **ESN**: This is a read-only field that displays the ESN of the HSM after you save the configuration and relaunch the editor. Infoblox strongly recommends that you verify the ESN displayed by the appliance with the one obtained from the HSM administrator to ensure that the appliance is communicating with the correct HSM.
4. Save the configuration.

### Monitoring the HSM Group

You can monitor the status of the HSM group and of individual modules in the group by navigating to the **Grid** tab > **HSM Group** panel. To view the status of each HSM, click the arrow beside the group name. This panel displays the following information:

- **Name**: The name of the HSM group or module.
- **Status**: The HSM group status displays the status for all the HSMs in the group. The status icon can be one of the following:
  - **Green**: All the HSMs in the group are functioning properly.
  - **Yellow**: At least one HSM in the group is not functioning properly.
  - **Red**: All the HSMs in the group are not functioning properly.
  - **Black**: The status of the HSM devices is unknown.

The status icon for each HSM can be one of the following:

- **Green**: The HSM is functioning properly. For SafeNet Luna SA 5 or SA 6 devices, the status icon can also display %x%used which refers to the storage capacity of the HSM partition that is assigned to the Grid. Note that when the capacity reaches 100%, new zone signings and key rollovers for existing zones cannot be performed.
- **Red**: The HSM is not functioning properly. For a SafeNet HSM, this indicates that the Grid Master was able to connect to the HSM, but no partition was assigned to the Grid Master.
- **Black**: The status of the HSM device is unknown.
- **FIPS**: This applies to a SafeNet HSM only. It indicates if the HSM is in FIPS compliant mode.
- **Comment**: Any comments that were entered about the HSM group.

You can also do the following in this tab:

- Sort the data in ascending or descending order by column.
- Print and export the data in this tab.

### Enabling HSM Signing

When you enable HSM signing, the HSM starts generating the DNSSEC keys at the next key rollover. For information about key rollovers, see **About Key Rollovers**. You can enable this feature at the Grid level only.
To enable HSM signing:

1. From the **Data Management** tab -> **DNS** tab, expand the Toolbar and click **Grid DNS Properties**.
2. In the **Grid DNS Properties** editor, Click **Toggle Expert Mode**, if the editor is in Basic mode, and then select the **DNSSEC** tab.
3. In the **DNSSEC** tab, select the **Enable DNSSEC** check box, if it is not selected, and then select the **HSM Signing** check box.
4. Complete the other fields described in **Configuring DNSSEC Parameters**. Note that Thales HSMs do not support DSA.
5. Save the configuration.

### Testing the HSM Group

After you configure the HSM group, you can test the HSM signing functionality of the group. Click **Test HSM Group** in the Toolbar, and then click **Yes** when the confirmation dialog displays. The appliance then executes the command to perform a signing test. The feedback panel displays the status of the test in the Grid Manager feedback panel.

### Synchronizing the HSM Group

You can click **Resync HSM Group** in the Toolbar to do any of the following:

- For a Thales HSM group, if the RFS security settings change use this function to have the appliance perform an RFS synchronization.
- For a SafeNet HSM group, use this function to synchronize the keys of the HSM members in the group.

### Configuring Grid Members to Support DNSSEC as Secondary Servers

Any Infoblox Grid member can function as a secondary server for DNSSEC signed zones. It can receive transfers of signed zones from the Grid Master or an external primary server, and from other secondary servers. It can also respond to queries for DNS data in DNSSEC signed zones for which it is a secondary server.

#### Configuring a Secondary Server for Signed Zones

The following are the tasks to configure an appliance as a secondary server for signed zones:

1. Enable DNSSEC on the appliance. For information, see **Enabling DNSSEC**.
2. Configure the appliance as a secondary server for the zone. For information, see **Specifying Secondary Servers**. If the primary server for the signed zone is external, then you must allow zone transfers to the secondary server.
3. For information, see **Enabling Zone Transfers**. If the primary server is the Grid Master, then the secondary server receives data through the Grid replication process by default.

### Configuring Recursion and Validation for Signed Zones

When you enable recursion on a Grid member and it receives a recursive query for DNS data it does not have, it queries remote name servers that you specified in the **Grid DNS Properties** or **Member DNS Properties** editor. It then includes the DNSSEC data it retrieved through recursion in its responses to clients that requested DNSSEC RRs. You can enable the appliance to validate the responses of these servers for certain zones. On the appliance, you specify the zones to validate and configure their DNSKEY records as trust anchors. When the appliance validates a response for a zone configured with a trust anchor or for any of its child zones, the appliance starts with the DNSKEY that you configured and proceeds recursively down the DNS tree.

In the example shown in 4820080, the following was configured on the NIOS appliance:

- Forwarder with the following IP address: 10.2.2.1
- Recursion was enabled
- DNSSEC and validation were enabled
- The corpxyz.com zone and its DNSKEY record were configured

*Figure 22.5*
Enabling Recursion and Validation for Signed Zones

The following are the tasks to enable recursion and validate recursively derived data:

1. Enable DNSSEC on the appliance. For information, see Enabling DNSSEC.
2. Enable validation and configure the trust anchor of each signed zone. For information, see You must configure at least one trusted DNSKEY RR.
3. Enable recursion on the appliance. For information, see Enabling Recursive Queries.
4. Complete any of the following:
   - Configure the forward, delegated, stub or root zones for the signed zones. For information, see Configuring Delegated, Forward, and Stub Zones and Creating a Root Zone.
   - Configure global forwarders and custom root name servers, if needed. For information, see Using Forwarders and About Root Name Servers.

Enabling DNSSEC Validation

To configure trust anchors and enable Infoblox name servers to validate responses:

1. Grid: From the Data Management tab, select the DNS tab. Expand the Toolbar and click Grid DNS Properties. Member: From the Data Management tab, select the Members tab -> member check box and click the Edit icon.
2. DNS View: From the Data Management tab, select the Zones tab -> dns_view check box and click the Edit icon. To override an inherited property, click Override next to the property to enable the configuration.
3. When the additional tabs appear, click DNSSEC.
4. In the DNSSEC tab, complete the following:
   - Enable DNSSEC validation: If you allow the appliance to respond to recursive queries, you can select this check box to enable the appliance to validate responses to recursive queries for domains that you specify. You must configure the DNSKEY RR of each domain that you specify.
   - Accept expired signatures: Click this check box to enable the appliance to accept responses with signatures that have expired. Though enabling this feature might be necessary to work temporarily with zones that have not had their signatures updated in a timely fashion, note that it could also increase the vulnerability of your network to replay attacks.
   - TrustAnchors: Configure the DNSKEY record that holds the KSK as a trust anchor for each zone for which the Grid member returns validated data. Click the Add icon and complete the following:
     - Zone: Enter the FQDN of the domain for which the member validates responses to recursive queries.
     - Secure Entry Point (SEP): This check box is enabled by default to indicate that you are configuring a KSK.
     - Algorithm: Select the algorithm of the DNSKEY record: RSA/SHA1(5), DSA (3), DSA/NSEC3 (6), RSA/MD5 (1), RSA/SHA1/NSEC3 (7), RSA/SHA-256 (8), or RSA-SHA-512 (10). This must be the same algorithm that was used to generate the keys that were used to sign the zones.
     - PublicKey: Paste the key into this text box. You can use either of the following commands to retrieve the key:
       - dig . dnskey +multiline
         The above command retrieves root zone keys and is the only public key you require for full chain of trust validation.
       - dig \[@server_address\] <zone> dnskey +multiline +dnssec
         The above command retrieves public keys from the zone you specify on the server and can be used if the parent zone is not signed.

Note that the aforementioned command provides you with a key you need to cross validate against other servers to ensure you have an identical key.
As an alternative, you can use http://data.iana.org/root-anchors/ to retrieve signed public keys. You can find the
trust anchors in formats like XML and CSR. For more information, refer to http://data.iana.org/root-anchors/draft-icann-dnssec-trust-anchor.txt.

- **Negative Trust Anchors:** Configure negative trust anchors to suppress DNSSEC validation for certain domains. Click the Add icon to add the domain name to the list. You can define negative trust anchors at the Grid level and override them at the member and DNS view levels. For more information about negative trust anchors, see 4820080.

To delete a negative trust anchor, select the check box adjacent to the **Zone** column and click the **Delete** icon.

5. Save the configuration and click **Restart** if it appears at the top of the screen.

**Defining Negative Trust Anchors**

A DNSSEC misconfiguration is not uncommon, and it can lead to failures in validating clients for particular domains. You can use negative trust anchors to enhance the deployment of DNSSEC validation even with misconfigured domains, as the administrator can enable DNSSEC validation without worrying about resolution failure for misconfigured signed domains that succeeds without DNSSEC validation. A negative trust anchor is a domain name for which DNSSEC validation must be suppressed even if the domain name is listed under a trust anchor.

You can define a negative trust anchor at the Grid level and override it at the member and DNS view levels. You can define negative trust anchors within a view or at the Grid level. If you define it at both levels, only the configuration with the view will be effective for the respective view.

For any specific domain name, negative trust anchors are mutually exclusive of trusted anchors; if a negative trust anchor is specified for a domain name, you cannot configure a trust anchor using the same name. Likewise, if a trust anchor is configured for a domain name, you cannot configure negative trust anchor using the same name.

Note that if there is a trust anchor for a specific name under a negative trust anchor, that trust anchor will re-enable DNSSEC validation for query names covered by the trust anchor. For example, if you configure trust anchors for "." and "example.com," and "com" is in the negative trust anchor list, queries for "www.example.com" are subject to DNSSEC validation, while DNSSEC validation will be suppressed for www.insecure.com, even if "." is listed in the trust anchor.

The appliance does not support automatic cleanup of negative trust anchors, nor does it provide any information about their expiration. Administrators must manually keep track of the status of domains listed as a negative trust anchor, and must remove them from the list as soon as the domains become DNSSEC signed correctly. Infoblox recommends that you do not use negative trust anchors, and rather disable DNSSEC validation, if the administrator is not familiar with negative trust anchors or is not able to maintain the negative trust anchors properly; careless use of negative trust anchors would rather hinder the deployment of DNSSEC, which is the opposite to the purpose of negative trust anchors. For more information about general technical details of negative trust anchors, refer to http://tools.ietf.org/html/draft-livingood-negative-trust-anchors.

Note the following about negative trust anchors:

- You must restart the DNS service when you modify the list of negative trust anchors.
- The appliance displays an error message if an entry is present in both the trust anchors and the negative trust anchors list for the same FQDN.
- The appliance displays an error message if the same FQDN is present multiple times in a negative trust anchor.
- When DNSSEC validation is suppressed due to a negative trust anchor, the corresponding response from the validating resolver does not include the AD bit.

**Applying Policies and Rules to DNS Queries that Request DNSSEC Data**

You can configure the NIOS appliance to always apply RPZ policies, DNS blacklists, or NXDOMAIN rules to DNS queries, regardless of whether the queries request DNSSEC data. You can also configure the appliance to generate synthesized AAAA records for DNS queries that request DNSSEC data.

**WARNING:** When you enable this feature, NIOS applies the selected policies and rules even when it responds to DNS clients that support DNSSEC EC. Note that responses to these clients may result in resolution failure. Infoblox recommends that you use caution when enabling this feature and DNSSEC validation at the same time.

To enable this feature, complete the following:

1. **Grid:** From the **Data Management** tab, select the **DNS** tab. Expand the Toolbar and click **Grid DNS Properties.**
2. **Member:** From the **Data Management** tab, select the **DNS** tab -> **Members** tab -> **member** check box and click the **Edit** icon.
3. **DNS View:** From the **Data Management** tab, select the **DNS** tab -> **default dns_view** tab -> **default dns_view** and click the **Edit** icon.
4. **Apply the selected policies/rules to queries requesting DNSSEC records** section, complete the following:
   - **Response Policy Zones (RPZ) policies:** Select this to apply RPZ policies to DNS queries that request DNSSEC data. You must install the RPZ license to view this check box. For more information, see About Infoblox DNS Firewall.
   - **Blacklist rules:** Select this to apply blacklist rules to DNS queries that request DNSSEC data. For more information, see About Blacklists.
   - **NXDOMAIN rules:** Select this to apply NXDOMAIN rules to DNS queries that request DNSSEC data. This check box is visible only if you install the Query Redirection license. For more information, see About NXDOMAIN Redirection.
   - **DNS64 Groups:** Select this to generate synthesized AAAA records for DNS queries that request DNSSEC data. For more information, see Enabling DNS64 Service.

The member and the DNS views inherit settings from the Grid, by default. To override the settings, click **Override.** You can...
override settings at the member and DNS view levels. To retain the same settings as the Grid, click *Inherit* at the member and DNS view level.

4. Save the configuration.

Chapter 23 Managing DNS Traffic Control

This chapter describes the Infoblox DNS Traffic Control solution. It provides guidelines about how to adjust DNS responses based on DNS query source IP, server availability, and network topology. It also describes the required objects in this process such as DTC (DNS Traffic Control) servers, pools, and LBDNs (Load Balanced Domain Names), and how to configure them to achieve the best load balancing results. It includes the following sections:

- **About DNS Traffic Control**
- **DNS Traffic Control Configuration Example**
- **DNS Traffic Control Querying Process**
- **Supported DNS Traffic Control Objects**
- **License Requirements and Admin Permissions**
- **Limitations of DNS Traffic Control**
- **Load Balancing Methods for DNS Traffic Control**
- **Configuring Topology Rules and Rulesets**
  - Defining Topology Rulesets
  - Viewing Topology Rulesets
  - Importing a Topology Database
  - Rebuilding EA Database
- **Using DNS Traffic Control Health Monitors**
  - Configuring HTTP Health Monitors
  - Configuring ICMP Health Monitors
  - Configuring PDP Health Monitors
  - Configuring SIP Health Monitors
  - Configuring SNMP Health Monitors
  - Configuring TCP Health Monitors
  - Managing Health Monitor Certificates
  - Modifying Health Monitors
  - Viewing Health Monitors
  - Deleting Health Monitors
- **Managing DNS Traffic Control Objects**
  - Configuring DNS Traffic Control Servers
  - Modifying DNS Traffic Control Servers
  - Configuring DNS Traffic Control Pools
  - Modifying DNS Traffic Control Pools
  - Configuring DNS Traffic Control LBDNs
  - Modifying DNS Traffic Control LBDNs
  - Testing DNS Traffic Control LBDNs
  - Viewing DNS Traffic Control LBDNs
  - Enabling or Disabling Traffic Control Objects
  - Deleting DNS Traffic Control Objects
- **Visualization for DNS Traffic Control Objects**
  - Working with the Visualization Panel
  - Adding Default Visualization

About DNS Traffic Control

Infoblox DNS Traffic Control (DTC) provides a load balancing solution by creating DNS responses based on DNS query source IP, server availability, and network topology. Through DTC, you can set up multiple global sites and configure supported objects and load balancing methods to direct DNS clients to the best available servers. For detailed information about how DNS Traffic Control handles DNS queries and responses, see [DNS Traffic Control Querying Process](#).

To use the DTC feature and bypass the standard DNS querying process, you must install the DNS Traffic Control license on designated Grid members. For information about license and admin requirements, see [License Requirements and Admin Permissions](#). Members that are not authoritative for zones or members that do not have the DTC license installed will not process DNS queries through DTC. However, the appliance can process DNS queries through DNS Traffic Control for secondary servers in the Grid using the data replication method. For more information about data replication, see [Replicating DNS Data](#).

DNS Traffic Control utilizes a load balancing mechanism to create DNS responses. It returns tailored DNS responses based on settings you configure for associated objects such as DTC servers, pools, and LBDNs. For more information about these objects, see [Configuring DNS Traffic Control LBDNs](#) and [Managing DNS Traffic Control Objects](#). You can configure load balancing methods for pools and LBDNs based on the source IP address and other criteria. For more information, see [Load Balancing Methods for DNS Traffic Control](#).

To ensure that DTC servers are reachable and can process DNS queries, you can configure health monitors that help you determine the availability of these servers. For more information, see [Using DNS Traffic Control Health Monitors](#).
After you have set up DNS Traffic Control for specific DTC objects, you can monitor their status as described in the section Viewing DNS Traffic Control Objects. You can also view a visualization of the hierarchy of DNS Traffic Control objects that you configured. For more information, see Visualization for DNS Traffic Control Objects.

You can enable or disable logging for DNS Traffic Control load balancing and health monitors. The appliance logs this information to the syslog. For more information, see Setting DNS Logging Categories.

You can configure the DNS Traffic Control properties for the Grid and Grid members. For more information, see Configuring DNS Traffic Control Properties.

**DNS Traffic Control Configuration Example**

*bookmark2090* illustrates the basic concept of DNS Traffic Control and how you can use it to direct DNS clients to the best available server using the Topology load balancing method. In the illustration, consider your company manages five data centers: California, Denver, New York, London, and Brussels. Each data center offers the same services and applications your users need. To optimize server utilization and minimize response time, you use DNS Traffic Control to provide DNS responses based on the source IP address and the geographic locations of your data centers.

You define your data centers as DTC server objects, and then add them to a pool based on their locations. Data centers in California, Denver, and New York go into Pool USA while London and Brussels go into Pool EU. You also create a topology ruleset containing geography rules that is used when you configure Topology as the load balancing method for your LBDN and pools. To ensure that your data centers are available, you also configure health monitors so that your pools can check the health of its DTC servers.

In DNS Traffic Control, you complete the following to set up the above configuration:

1. Define a geography rule for the topology ruleset, as described in Configuring Topology Rules and Rulesets.
2. Configure each data center as a DTC server object, as described in Configuring DNS Traffic Control Servers.
3. Configure health monitors that NIOS will use to check the availability of DTC servers, as described in Using DNS Traffic Control Health Monitors.
4. Create two pools (USA and EU), which group your servers by geographical locations, configure health monitors that you created earlier, and then select Topology as the load balancing method. For information, see Configuring DNS Traffic Control Pools.
5. Define an LBDN and select Topology as the load balancing method and then associate it with a DNS zone. The appliance can then match the geography of the source IP addresses and direct the client to the best available server. For information, see Configuring DNS Traffic Control LBDNs.

**Figure 23.1 DNS Traffic Control Example**

To achieve load balancing results for DNS Traffic Control, you can configure DTC objects in the following order:

1. Create DNS Traffic Control servers for each data center or server you want to manage. For information, see Configuring DNS Traffic Control Servers.
DNS Traffic Control Querying Process

DNS Traffic Control handles a DNS query if the query name belongs to a zone for which the appliance is authoritative and matches an LBDN that is linked to the respective zone. Otherwise, the appliance processes DNS queries normally using the standard DNS query processing.

If you have configured persistence for DTC LBDN and the DTC cache contains a previous response for the same client, then DTC returns the cached response to the respective client. Otherwise, the DNS Traffic Control querying process first selects an LBDN, a pool, and then a specific server from that pool. A DNS record is synthesized from the address of the selected server and returns only DTC LBDN records to the client. Note that the configured DNS records are obscured by the DTC LBDN records. The obscured records are indicated by a strikethrough. For example, an obscured A record appears as A Record in Grid Manager.

When all the pools associated with the LBDNs are unavailable, the appliance returns DNS data for the zone. For information about how to configure availability and topology rules, see Configuring Topology Rules and Rulesets.

Following is a brief description of the DNS Traffic Control querying process:

1. The DNS Traffic Control querying process first checks an LBDN's DTC cache to verify if a response is available for the same client, same query and if the server in the cached response is online. If these conditions match, it returns the cached response to the client and refreshes the cache expiry time.
2. If the response is not available in the DNS Traffic Control cache, the DNS Traffic Control querying process occurs as follows:
   - Based on the FQDN in the request, the DNS Traffic Control querying process selects a matching LBDN based on its associated zone and pattern.
   - Based on the selected LBDN load balancing method, the DNS Traffic Control querying process selects an available pool. It does not select pools that are not available or do not have online servers associated with it. If pools are not available for the selected LBDN, the DNS Traffic Control querying process fails to determine the result.
   - After selecting a pool, the DNS Traffic Control querying process selects a server from the pool, based on the load balancing method that you have selected for the respective pool. The DNS Traffic Control querying process uses the preferred load balancing method of the pool by default and the alternate method only if the preferred method fails to return a result.
   - If the DNS Traffic Control querying process fails to determine a result, then the DNS server responds to the client with the matching DNS records configured for the respective zone. If matching DNS records are not configured, it returns an empty result.

You can enable or disable the DTC to DNS fall through in the Grid DNS properties.

Supported DNS Traffic Control Objects

You can configure the following DNS Traffic Control objects in the Grid:

- **Server**: DNS Traffic Control synthesizes DNS records for the servers. For information about how to add and modify servers, see Configuring DNS Traffic Control Servers.
- **Pool**: A pool is a collection of servers that you can put together as possible responses to queries. For information about how to add and modify load balancing pools, see Configuring DNS Traffic Control Pools.
- **LBDN**: A DTC LBDN is a load balanced domain name object that is used by DNS Traffic Control to process DNS queries for load balanced resources. For more information about how to add and modify LBDN objects, see Configuring DNS Traffic Control LBDNs.

License Requirements and Admin Permissions

The DNS Traffic Control works as an add-on feature for the DNS service in the NIOS appliance. In order to use it, install the DNS and DNS Traffic Control licenses on the appliance. You can add the DNS Traffic Control license only when you have installed the DNS license. After you add the license, the feature becomes available to you in Data Management -&gt; DNS -&gt; Traffic Control.

The DNS Traffic Control feature starts, stops, or restarts with the DNS service. You may need to restart the DNS service after you make configuration changes. When you click Restart at the top of the screen, the DNS Traffic Control service takes some time to update the configuration and the status of LBDNs, pools and servers on the appliance. For more information about how to install licenses, see Managing Licenses.

The appliance creates a new role, DTC Admin, when you install the DNS Traffic Control license. For more information about how to define permissions, see About Admin Roles.

- You can update, add, or delete LBDNs if you have read/write permission on All DTC LBDNs, but you need additional permissions to link them to a zone.
- You must have read/write permission on All DTC LBDNs to modify an LBDN if a configuration change results in a deletion of LBDN records.
- You must have read/write permission on both All DTC LBDNs and All DTC LBDN Records to modify LBDN patterns that might result in...
the creation of new LBDN records.
- Administrators who have access to set up zones have read/write access to their LBDN records. The LBDN records permission is similar to other zone record permissions.
- When you link an LBDN to a zone, you must have both read-only permission on All DTC LBDNs and read/write permission on the LBDN record of the zone.
- You must have read/write permission on All DTC LBDNs to disable an LBDN. This implicitly disables associated LBDN records from the associated zones and does not require an LBDN record permission.
- You must have read/write permission on All Topology Databases to upload a MaxMind GeoIP location database. To modify a rule in the topology ruleset, you must have read/write permission on All DTC Topologies.
- To create and modify DTC pools, you must have read/write permission on All DTC Servers.
- You must have read/write permission on All DTC Monitors, All DTC Certificates, and All DTC Topologies to create and modify DTC monitors, certificates and topologies respectively.

For more information about defining global permissions, see Defining Global Permissions.

Limitations of DNS Traffic Control

- A member will return DNS Traffic Control results for a zone only if the member is a Grid primary, or a Grid secondary that is using database replication. DNS Traffic Control results are not produced for zones using AXFR, regardless of whether or not the primary member is in the Grid.
- The DNS Traffic Control querying process is not supported for recursive queries.
- The DNS Traffic Control does not support the Global application of an LBDN pattern against all queries. The appliance returns a result only if the query resolves to an authoritative zone to which an DNS Traffic Control LBDN is explicitly linked.
- You can use the IDN converter for conversion, but the appliance supports manually encoded puny code as an LBDN pattern.
- You cannot install the DNS Traffic Control license on the Infoblox 4030 appliance.
- DNS Traffic Control health monitoring does not monitor servers if the server has IPv4 and/or IPv6 addresses and the health monitoring interface on the Grid member does not have the corresponding IP address type. The appliance sets the status as unknown for such IPv4 and IPv6 addresses. In addition, the appliance may return a timeout error while loading the Traffic Control tab in Grid Manager if you have configured health monitoring for a lot of DTC servers.
- Infoblox does not support running DNS Traffic Control on the TE-810 and TE-820 appliances.

Load Balancing Methods for DNS Traffic Control

You can define the following load balancing methods:

<table>
<thead>
<tr>
<th>Load Balancing Method</th>
<th>LBDN</th>
<th>Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Available</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>Global Availability</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Round Robin</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Ratio: Fixed</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Ratio: Dynamic (Round Trip Delay)</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>Ratio: Dynamic (SNMP)</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>Topology</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

Based on the load balancing method defined for an LBDN, the DNS Traffic Control selects an available pool. Based on the method selected for a pool, it selects an available server.

The following is a description of the load balancing methods with examples for pools or LBDNs:

- Using the All Available method, the appliance responds to the query with all the available servers in the DTC pool for the appropriate record type. The responses are returned in the same order in which the servers are listed in the DTC pool, eliminating the unavailable servers.

Consider the following example for all available records load balancing method with an LBDN x.abc.com:

- Pool= Pool_1; load balancing method= all available records; health check= HTTPS
  10.10.1.1; Availability = up
  2001:db8:a22:a00::29; Availability = up
  10.10.2.2; Availability = down
  2001:db8:a22:a00::32; Availability = up
  10.10.3.3; Availability = up

In this example, the appliance responds with 10.10.1.1, 10.10.3.3 for each A record query. For each AAAA record query, NIOS responds
with 2001:db8:a22:a00::29, 2001:db8:a22:a00::32. The unavailable servers are eliminated. Note that the system considers only the order of the servers in the DTC pool and ignores the weight of available servers.

- **Using the Global Availability** method, the appliance creates the response to the query, so that the clients are directed to the first available pool and server.

  Consider the following example for global availability load balancing method with an LBDN x.abc.com:

  - **Pool = Pool_1; load balancing method = global availability; health check = HTTPS 10.10.1.1**
  - 10.10.2.2
  - 10.10.3.3
  
  - **Pool = Pool_2; load balancing method = global availability; health check = HTTPS 10.10.4.4**
  - 10.10.5.5
  - 10.10.5.5

  In this example, the appliance always responds with 10.10.1.1 (A record) for all x.abc.com queries assuming that all servers are available. The DNS Traffic Control LBDN determines which pool to use based on the health check response and adjusts the response accordingly. The appliance responds with 10.10.4.4 from Pool_2 if health check for all servers associated with Pool_1 fails.

- **Using the Ratio: Fixed** method, NIOS adjusts the response to the query so that the clients are directed to servers in a pool or among pools. When multiple pools or servers are configured, the appliance uses the weighted round robin method, a load-balancing pattern in which requests are distributed among several pools or servers based on a weight assigned to each pool or server. Note that the system considers the weight of available servers only.

  Consider the following example for ratio load balancing method with an LBDN x.abc.com, load balancing method = Ratio and two linked pools: Pool_1 with weight = 70 and Pool_2 with weight = 30.

  - **Pool = Pool_1; load balancing method = ratio; health check = HTTPS 10.10.1.1; Weight = 50**
  - 10.10.2.2; Weight = 2
  - 10.10.3.3; Weight = 25

  - **Pool = Pool_2; load balancing method = ratio; health check = HTTPS 10.10.4.4; Weight = 50**
  - 10.10.5.5; Weight = 25
  - 10.10.5.5; Weight = 25

  In this example, the appliance responds 70% of the time with a server associated with Pool_1. Within Pool_1, it responds with 10.10.1.1 address 50% of the time.

- **Using the Ratio: Dynamic** method, the appliance weights the DTC servers dynamically based on round trip delay or SNMP health monitor data. You can use one of the following options:

  - **Round trip delay:** Based on the round trip delay from the DTC member that received a client’s DNS request, the system sends clients to the server with the minimal latency time, i.e. the closest one. You need a pre-configured health monitor for this load balancing method.

    For example:

    - Server A latency = 25 ms
    - Server C latency = 18 ms
    - Server D latency = 50 ms

    In this case, the traffic distribution is as follows:

    - Server A = 0%
    - Server C = 100%
    - Server D = 0%

  - **SNMP:** Based on data from the SNMP monitor associated to the server, for example, CPU or memory utilization, the system sends clients to the server with the lowest load. For this load balancing method, you need a pre-configured SNMP health monitor with a required metric to be tracked. The metric is set through an object identifier (OID) in the monitor properties. This method supports only OIDs for which the server can return an integer value.

    The value of the monitored metric defines how the traffic is directed. By default, the servers with the highest metric values receive the client requests. There may be cases when your selected metric reflects server availability in the opposite way, that is, the lowest metric values indicate available servers. For such cases, you can invert the value of the OID, that is, of the monitored metric, and have the traffic directed to the lowest-rated servers.

    You can select to weight servers by either priority or ratio. In case of priority, traffic is directed towards the servers that report the best metric values, other servers being bypassed. In case of ratio, traffic is distributed across all servers based on the values of the monitored metric for each of them. If a health check for a server is failed, the server is excluded from the load balancing.

    Consider the following example where the CPU utilization metric is used for server monitoring:

    - Server A CPU utilization = 90%
Server C CPU utilization = 50%
Server D CPU utilization = 10%

With normal dynamic weights, the distribution is as follows:

- Server A 60% (calculated as 90 / (10 + 50 +90) = 90/150 = 0.6)
- Server C 33% (calculated as 50 / (10 + 50 +90) = 50/150 ~ 0.33)
- Server D 7% (calculated as 10 / (10 + 50 +90) = 10/150 ~ 0.066)

This means that the most loaded server will receive most requests than the less loaded one. For this case, the metric should be inverted to reflect server availability appropriately:

- Server A 8% (calculated as 1/90 / (1/90 + 1/50 + 1/10) = 0.011/0.131 ~ 0.08)
- Server C 15% (calculated as 1/50 / (1/90 + 1/50 + 1/10) = 0.02/0.131 ~ 0.15)
- Server D 77% (calculated as 1/10 / (1/90 + 1/50 + 1/10) = 0.1/0.131 ~ 0.77)

**NOTE:** You can see traffic distribution percentage across members in pools and servers based on selected load balancing methods in the visualization panel. For information, see Visualization for DNS Traffic Control Objects on page 1087.

- Using the **Round Robin** method, the appliance returns servers sequentially and cyclically. Consider the following example for round robin load balancing method with an LBDN x.abc.com:
  - Pool = Pool_1; load balancing method = Round Robin; health check = HTTPS 10.10.1.1;
  - 10.10.2.2;
  - 10.10.3.3;

  In this example, NIOS responds with a server associated with Pool_1. Within Pool_1, it responds sequentially:
  - Time 1: Response = 10.10.1.1
  - Time 2: Response = 10.10.2.2
  - Time 3: Response = 10.10.3.3
  - Time 4: Response = 10.10.1.1
  - Time 5: Response = 10.10.2.2
  - Time 6: Response = 10.10.3.3

- Using the **Topology** method, the appliance applies a predefined geographic mapping method and evaluates user-defined geography, subnet, or extensible attribute rules sequentially. Geographical locations for the geography rules are provided through an external topology database. The appliance supports the MaxMind GeoIP2 City or Country database and the MaxMind GeoLite2 City or Country database. For more information, see the following section, Configuring Topology Rules and Rulesets.

### Configuring Topology Rules and Rulesets

A topology rule maps a client IP address to a DNS Traffic Control pool or server. To use Topology as the load balancing method for a pool or an LBDN, you must define a topology ruleset containing at least one rule. The rulesets are configured globally. When the DNS Traffic Control returns a response, it evaluates the list of rules in the topology ruleset in order and uses the first match with an available destination. The method fails if there are no matches.

You can define the following topology rules in a ruleset:

- Extensible Attribute rule
- Subnet rule
- Geography rule

The destination for a topology ruleset is either a server or a pool. An LBDN can use only topology rulesets with a pool as the destination. A pool can use only topology rulesets with a server as the destination.

You can also use CSV import to import rules into NIOS.

### Defining Topology Rulesets

A topology ruleset can contain multiple rules. The rules in a topology ruleset must use the same destination type. Multiple LBDNs or pools can reuse a topology ruleset.

Each server that you use as a destination in the topology must exist in every pool that is using the topology. When you select Topology as a load balancing method for a pool, you can select one of these rulesets for the topology rules. The ruleset can be a combination of extensible attribute, subnet, and/or geography rules.

Note the following about extensible attribute, subnet, and geography source matches:

- A rule with an extensible attribute source matches if a client query comes from the network that has the specified set of extensible attributes, i.e. extensible attributes you specify when you create a rule.
- A rule with a subnet source matches if the subnet contains the client IP address.
- A rule with a geography source label matches if the client IP address and geography source label matches corresponding information in the MaxMind location database.

Note the following information about rules and rulesets:
When you upload a new MaxMind location database or restore a backup, the appliance does not automatically remove rules that contain invalid labels. Instead, it marks the rules with labels that do not exist in the database as invalid. The appliance ignores these rules during the querying process, and you cannot save the configuration if it is modified, but you can use the existing configuration.

The appliance checks specific combinations of labels when the rules use multiple conditions. For example, if you have a rule with the source types Country = Canada and City = Vancouver and you change the Country source type to Russia, then the City source type is cleared and the selector resets to contain only known cities in Russia. This is applicable for both geography and extensible attribute rules.

An example of valid source types:

<table>
<thead>
<tr>
<th>Continent</th>
<th>Country</th>
<th>Subdivision</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Canada</td>
<td>Any</td>
<td>Vancouver</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Vancouver</td>
</tr>
<tr>
<td>North America</td>
<td>Any</td>
<td>Any</td>
<td>Vancouver</td>
</tr>
<tr>
<td>North America</td>
<td>USA</td>
<td>Washington</td>
<td>Vancouver</td>
</tr>
</tbody>
</table>

When rules have multiple source conditions, the client must match all conditions for the rule to execute.

A ruleset may have multiple subnet rules and the subnets may overlap. Similarly, a ruleset may have multiple geography rules and the matches may overlap. Similarly, a ruleset may have multiple extensible attribute rules and the matches may overlap. During the querying process, the rules in a topology ruleset are evaluated in order. For example, if you configure subnet rules where #1 is 10.10.0.0/16 and #2 is 10.0.0.0/8, both are considered valid in the appliance.

To define a ruleset, complete the following:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab, and then click Manage Topology Rulesets in the Toolbar.
2. In the Topology Manager window, click the Add icon.
3. In the Ruleset wizard that appears, complete the following:
   - **Name**: Enter a name for the ruleset.
   - **Destination Type**: Select a destination type, Pool or Server. Rulesets with the Pool destination type can only be used by LBDNs. Rulesets with the Server destination type can only be used by pools. You cannot change the destination type if the ruleset contains any rules.
   - **Comment**: Enter additional information about the ruleset.
   - **Rules**: You can define multiple extensible attribute rules, subnet rules, and geography rules in the ruleset. Click the arrow next to the Add icon and select either Extensible Attribute Rule, Subnet Rule, or Geography Rule.
     - When you select Extensible Attribute Rule, Grid Manager displays the following:
       - **Source Type**: Define up to four extensible attributes to use as the source type for the EA topology ruleset. To define extensible attribute source types for the topology rules, see Configuring Grid DNS Traffic Control Properties. Note that "Any" matches any value. There must be at least one source type with a specific value (the value is not "Any"). When a source type uses "does not equal" as the operator, it must be the lowest level source type (most specific). For example, with Continent/Country/Subdivision/City, City is the most specific source type.
       - **Destination**: Click Select to select a destination. The appliance displays the DTC Pool Selector dialog box when you have selected the Pool destination type and displays DTC Server Selector dialog box when you have selected the Server destination type. Click a specific pool or server to select it. Note that if there is only one pool or server, no dialog box is displayed when selecting the destination.
     - Click Add to add the source. The appliance displays the following information in the Rules table:
       - **Source**: The values of extensible attributes that you specified.
       - **Destination**: The destination that you selected.
       - **ValidSource**: After you save the ruleset, the value is set to Yes if the extensible attributes exist in the EA database.

   **Note**: The source must be valid when creating a ruleset. It can become invalid when a new topology database no longer contains the source.

   - **Order**: Displays the order of the rule in the ruleset.
   - When you select SubnetRule, Grid Manager displays the following:
     - **SourceSubnet**: Select a value from the drop-down list. You can either select equals or doesnotequal and specify a subnet IP address or click Select and choose a network from the NetworkSelector dialog box. Note that "Any" matches any value. There must be at least one source subnet with a specific value (the value is not "Any"). When a source subnet uses "does not equal" as the operator, it must be the lowest level source subnet (most specific).
     - **Destination**: Click Select to select a destination. The appliance displays the DTC PoolSelector dialog box when you have selected the Pool destination type and displays DTC ServerSelector dialog box when you have selected the Server destination type. Click a specific pool or server to select it. Note that if there is only one pool or server created, no dialog box is displayed when selecting the destination.
Click Add to add the source. The appliance displays the following information in the Rules table:

- **Source:** The subnet address that you specified.
- **Destination:** The destination that you selected.
- **Valid Source:** For a subnet rule, the rule is always marked as valid after you save the ruleset.
- **Order:** Displays the order of the rule in the ruleset.

• When you select **Geography Rule**, Grid Manager displays the following:
  - **Source Type:** Select a source type.
  - **Continent:** Select a continent from the drop-down list. You can also enter the first few characters of the continent to match an item in the database.
  - **Country:** Select a country from the drop-down list. You can also enter the first few characters of the country to match an item in the database.
  - **Subdivision:** Select a subdivision from the drop-down list. You can also enter the first few characters of the subdivision to match an item in the database.
  - **City:** Select a city from the drop-down list. You can also enter the first few characters of the city to match an item in the database. The drop-down list has paging controls to page through the available values.
  - **Destination:** Click to select a destination. The appliance displays the DTC Pool Selector dialog box when you have selected the Pool destination type and the DTC Server Selector dialog box when you have selected the Server destination type. Click a specific pool or server to select it. Note that if there is only one pool or server created, no dialog box is displayed when selecting the destination.

Click Add to add the source. The appliance displays the following information in the Rules table:

- **Source:** The subnet address that you specified.
- **Destination:** The destination that you selected.
- **Valid Source:** After you save the ruleset, the value is set to Yes if the labels exist in the MaxMind location database.
- **Order:** Displays the order of the rule in the ruleset.

• **Default destination if none of the above rules match (optional):** Click Select to select the default destination if none of the above rules match. The appliance displays the DTC Pool Selector dialog box when you have selected the Pool destination type and displays the DTC Server Selector dialog box when you have selected the Server destination type. Click a specific pool or server to select it. You can click Clear to remove the selected pool or server. Note that you can select a default destination even if there are no rules defined in the Rules table.

4. If necessary, modify the order of rules in the table. You can do so by editing the value in the Order column or using the arrows on the left side of the table.

5. Click Next.

6. Define the extensible attributes. For information, see Using Extensible Attributes.

7. Click Next to schedule change. In the ScheduleChange panel, click Now to immediately execute this task. Or click Later to schedule this task, and then specify a date, time, and time zone.

8. Click Save & Close.

**Note:** After making changes to the extensible attributes, you may need to rebuild the topology EA database. For more information, see Rebuilding EA Database.

### Viewing Topology Rulesets

To view topology rulesets, navigate to the Data Management tab -> DNS tab -> Traffic Control tab, and then click Manage Topology Rulesets in the Toolbar. The Topology Manager lists the configured rulesets, their destination types, sites, and comments.

You can do the following:

- **Add new rulesets.** To add a new ruleset, click the Add icon. For more information, see Defining Topology Rulesets.
- **Edit a ruleset by clicking the check box next to the ruleset name and clicking the Edit icon.** You can modify the following in the Ruleset editor:
  - In the General Basic tab, you can do the following:
    - Add new rules to the ruleset. Click the arrow next to the Add icon and select either Extensible Attribute Rule, Subnet Rule, or Geography Rule. For more information, see Defining Topology Rulesets.
    - Modify rules in the ruleset. To edit an existing rule, select the check box of the required rule in the Rules table and click the Edit icon. When finished with editing, click Save above the Rules table. For more information, see Defining Topology Rulesets.
    - Delete existing rules from the ruleset. Select the check box of the required rule in the Rules table and click the Delete icon.

**Note:** You can modify the destination type only if there are no rules in the ruleset.
In the **ExtensibleAttributes** tab, you can add new or edit existing extensible attributes. For information, see *Using Extensible Attributes*.

- Delete a ruleset or schedule the deletion for a later time. To delete a ruleset, select the check box next to its name and click the arrow next to the Delete icon. To delete the object immediately, select **Delete**. To schedule the deletion, click **Schedule Delete**. For more information, see *Scheduling Deletions*.
- Export topology rulesets. To export the entire list of rulesets in a format that can be imported, click the Export icon and choose **Export data in Infoblox CSV Import format**. To export all data that is currently visible in the Topology Manager, click the Export icon and choose **Export visible data**.
- Print the data that is currently visible in the Topology Manager. Click the Print icon to print.

**Importing a Topology Database**

The DNS Traffic Control license includes a MaxMind location database that is deployed when you enable DNS Traffic Control. Note that only a single MaxMind location database can be present on the Grid at a time. The MaxMind location database contains various geography locations that can be used when you define a geography rule. NIOS supports both paid GeoIP2 and free GeoLite2 MaxMind location databases. The GeoLite2 MaxMind Country database is shipped with the NIOS appliance. The MaxMind location database is static over the lifetime of the querying process until you import a new database and restart services.

When you import a new MaxMind location database, the appliance replaces the existing database. You can import MaxMind location databases that are in MMDB or CSV format. To view the current version of the database, click **Current Version**.

You can import a ready-to-use MaxMind location database or create your own ZIP file containing multiple CSV files. To import a MaxMind location database or to view the current version of the database, complete the following:

1. From the **Data Management** tab, select the **DNS** tab, and then select the **Traffic Control** tab.
2. Click the arrow next to the **Topology Database**, and then select **Import GeoIP Database** from the drop-down list.
3. In the **Import Topology Database** wizard, complete the following:
   - **File**: Click **Select** and navigate to the MaxMind location database.
   - **Upload**: Click **Upload** to import the MaxMind location database.
4. In the Toolbar, click the arrow next to **Topology Database**, and select **Current Version** from the drop-down list to view the details of the imported MaxMind location databases. In the Geography section, Grid Manager displays the database type, build date, build version, and the date and time when the database was deployed to the Grid Master.

**Note:** The latest database version may not be deployed on all DTC members. To view the current deployed versions, select **Data Management** - > **DNS** - > **Members**.

To create a custom database in a ZIP file:

1. Create a directory with CSV files and name them using the following pattern:
   
   
   
   
   {Product}-{Content}-{Blocks-or-Locations}-{version-or-localization}.csv.

   Only the three CSV files matching these patterns are suitable for the import:

   - {Product}-{Content}-Blocks-IPv4.csv
   - {Product}-{Content}-Blocks-IPv6.csv
   - {Product}-{Content}-Locations-en.csv

   For example:

   GeoLite2-City-Blocks-IPv4.csv
   GeoLite2-City-Blocks-IPv6.csv
   GeoLite2-City-Locations-ru.csv

   or

   GeoIP2-Country-Blocks-IPv4.csv
   GeoIP2-Country-Blocks-IPv6.csv
   GeoIP2-Country-Locations-en.csv

   where

   - “GeoLite2” and “GeoIP2” correspond to {Product}
   - “City” and “Country” correspond to {Content}
   - “IPv4” and “IPv6” correspond to {version}
   - “ru” and “en” correspond to {localization}
Note: The Locations file and at least one of the Blocks files must exist or the import fails. Also, all of these files must have identical {Product}-{Content} pairs or the import fails. You can use a ready-to-use MaxMind location database as an example.

2. You can add multiple CSV files for different localizations to your ZIP file. Use the following naming pattern:

{Product}-{Content}-Locations-{localization}.csv.

For example:

- GeoLite2-City-Locations-ru.csv
- GeoIP2-City-Locations-de.csv
- GeoIP2-Country-Locations-en.csv

3. Add the directory with the CSV files to a ZIP file. The name of the ZIP file you upload and the name of the directory in the ZIP file are not significant. The ZIP file should contain only one directory and no subdirectories. Any files in the ZIP file with an extension different from .csv are ignored.

4. Import the ZIP file to Grid Manager as described above.

Note: The Country database does not support 'subdivision' labels and importing it invalidates all existing rules that use 'subdivision' labels.

**Rebuilding EA Database**

Unlike the GeoIP database, the EA database is not imported externally but configured within the system. After making changes to extensible attributes, Grid Manager offers you to rebuild the DNS Traffic Control Topology Database. You can use the banner that appears at the top of the screen and click Rebuild to rebuild the database immediately. Or, you can click Ignore to rebuild the database later in the Traffic Control tab. Clicking Ignore applies to all changes that require a rebuild of the EA database. The EA database rebuild is ignored for the duration of the user session.

To rebuild the EA database:

1. From the Data Management tab, select the DNS tab, and then select the Traffic Control tab.
2. In the Toolbar, click the arrow next to the Topology Database and select Rebuild EA Database -> Rebuild or Schedule Rebuild.
3. In the Rebuild EA Database dialog box, select Yes to rebuild the database or No to discard the rebuild. To schedule the rebuild task, in the Rebuild EA Database Schedule dialog box, specify a date, time, and time zone.

To view the current version of the EA database, click Topology Database -> Current Version in the Toolbar. Grid Manager displays the database build date and its last rebuild status in the Extensible Attributes section.

Note: The latest database version may not be deployed on all DTC members. To view the current deployed versions, select Data Management -> DNS -> Members.

**Using DNS Traffic Control Health Monitors**

Health monitors determine the availability of DTC servers. You associate health monitors with pools. Every health monitor checks each server that is associated with the pool. Additionally, if you use multi-tier architecture, you can assign health monitors to individual IP addresses of a DTC server. You can use pre-defined health monitors or create custom monitors.

You can configure health monitors of the following types:

- HTTP health monitors. See Configuring HTTP Health Monitors.
- ICMP health monitors. See Configuring ICMP Health Monitors.
- PDP health monitors. See Configuring PDP Health Monitors.
- SIP health monitors. See Configuring SIP Health Monitors.
- SNMP health monitors. See Configuring SNMP Health Monitors.
- TCP health monitors. See Configuring TCP Health Monitors.

When you install the DNS Traffic Control license, each Grid member that is associated with an LBDN independently monitors the health of a server. The appliance resolves the server FQDN using the system resolver. The appliance performs a health check on both the IPv4 and IPv6 addresses. If the member does not have the same IP address types as the server or if the DNS name resolution for A or AAAA records fail to return results, the corresponding health check is considered to be a failure. The appliance caches the addresses that are resolved. Note that monitoring is done by each Grid member that has a DNS Traffic Control license and is associated with a zone that has an LBDN record. This implies that firewall policies should be such that the member can reach every server it is monitoring. Otherwise, DNS Traffic Control cannot direct responses to servers that are not accessible.

By default, all monitor checks are initiated from the virtual interface of the member that is performing the health check. If the monitored server has only an IPv4 or IPv6 address, then the interface must have the corresponding IP address type.

You can configure the DTC monitor source to use the VIP, MGMT, LAN2 (WHERE), or ANY (normal routing) NIOS network interface, or one of the loopback additional IP addresses for the Grid member. You can configure the loopback IP address in the Grid member editor or network configuration.
The status of a DTC server for a specific pool depends upon the status of all the health monitors that are checking it. The status of a pool depends upon the status of all the servers in the pool. The status of an LBDN depends upon the status of all the pools assigned to the LBDN.

For the HTTPS and SIP monitor types, you can upload client certificates and associate them with the monitors to provide when connecting to a DTC server. For information, see Managing Health Monitor Certificates.

Vice versa, DTC servers provide certificates to authenticate themselves to the HTTPS and SIP monitors. You enable DTC server certificate validation when configuring HTTPS and SIP health monitors.

### Configuring HTTP Health Monitors

An HTTP health monitor sends either an HTTP or HTTPS request to the server. The health monitor then examines the response received from the server. The validation is successful if the server returns a response with the expected result code.

The HTTP/HTTPS monitor can validate the response code and response content. The response content is checked only when the response code is valid. You can define regular expressions to use for the response content check. The supported regular expression syntax is POSIX Extended Regular Expression. For information, see Appendix D, “Regular Expressions”.

If the DTC server certificate validation is enabled in the HTTPS health monitor, you can use the Server Name Indication (SNI) feature for remote DTC servers. SNI is an extension to the TLS computer networking protocol by which a client indicates which hostname it attempts to connect to at the start of the handshaking process. This allows a server to present multiple certificates on the same IP address and TCP port number. Thus, multiple secure (HTTPS) websites (or any other service over TLS) can be served off the same IP address without all those sites having to use the same certificate.

After you configure an HTTP/S monitor, you can test its performance. See Testing HTTP Health Monitors.

**Note:** The HTTP health monitor does not support user name or password authentication.

To configure an HTTP health monitor, complete the following:

1. From the **Data Management** tab, select the **DNS** tab -> **Traffic Control** tab, and then click **Manage Health Monitors** in the Toolbar.
2. In the Health Monitors Manager, click the arrow next to the Add icon and select **HTTP Health Monitor**.
3. In the **HTTP Health Monitor Wizard**, complete the following:
   - **Name**: Enter a name for the HTTP monitor.
   - **Interval (seconds)**: Enter the interval value in seconds. The interval value is measured from the end of the previous monitor cycle. The default value is five.
   - **Timeout (seconds)**: Enter the timeout value in seconds. The monitor waits for the number of seconds that you specify after sending a response. If it does not receive a response within the number of seconds that you specify, then the appliance considers this check as failed. The monitor discards any response it receives after the timeout. The default value is 15.
   - **Retry Up Count**: Enter a retry up count. When you specify a value, the appliance checks whether the server is up based on the following: interval*retry up count. For example, if you specify the interval as five seconds and the retry up count as 10 seconds, then the appliance tries to connect to the server every five seconds for a period of 50 seconds. If the server is down initially, the appliance tries to connect to the server for a period of 50 seconds in sequence. When the connection is successful, the HTTP monitor considers the server to be up. If the server is unavailable for an entire period of 50 seconds, the appliance considers this connection as a failure.
   - **Retry Down Count**: Enter a retry down count. The HTTP monitor considers the server unavailable only if the server is unavailable during the period: interval*retry down count. For example, if you specify the interval as five seconds and the retry down count as 10 seconds, then the appliance checks if the server is unavailable for 50 seconds in sequence. If the server is unavailable for an entire period of 50 seconds, the appliance considers the server to be down.
   - **Comment**: Enter information about the HTTP monitor.
4. Click **Next** and complete the following:
   - **Port**: For HTTP, the appliance displays port number 80 by default. If you select **Use HTTPS**, the appliance displays 443 by default.
   - **Use HTTPS**: Select the check box to enable HTTPS. Specify any of the following options that become available when you select to use HTTPS:
     - **Client Certificate**: Optionally, you can select a certificate to use while opening the SSL connection for HTTPS. The monitor does not inspect or validate the server certificate, if any. For information about how to upload certificates, see Managing Health Monitor Certificates.
     - **Ciphers**: Specify a list of SSL ciphers in an OpenSSL format. You can specify cipher texts up to 1024 characters. The client certificate and cipher list are only used for HTTPS transport. The following example commands list some available ciphers:

**Example 1:**

```bash
$ openssl ciphers 'HIGH:!DES'
DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:
DHE-DSS-CAMELLIA256-SHA:ADH-AES256-SHA:ADH-CAMELLIA256-SHA:AES256-SHA:
CAMELLIA256-SHA:PSK-AES256-CBC-SHA:EDH-RSA-DES-CBC3-SHA:
EDH-DSS-DES-CBC3-SHA:ADH-DES-CBC3-SHA:DES-CBC3-SHA:DES-CBC3-MD5:
PSK-3DES-EDE-CBC-SHA:KR5-DES-CBC3-SHA:KR5-DES-CBC3-MD5:EDH-RSA-AES128-SHA:
DHE-DSS-AES128-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:
```

**Example 2:**

```bash
$ openssl ciphers 'DEFAULT:!EDH+eRSA'
DHE-DSS-AES256-SHA:DHE-DSS-CAMELLIA256-SHA:AES256-SHA:CAMELLIA256-SHA:
```
Note: The DHE cipher list family ("Diffie-Hellman key agreement" plus "RSA authentication") could consume excessive CPU and is excluded from the defaults used by DNS Traffic Control health monitors. Although you can enable these ciphers by explicitly configuring them in the cipher list for HTTPS and SIP monitors, you should be aware that doing so will increase CPU usage. Since health monitoring in general does not require high security, Infoblox recommends that you enable these ciphers only for target servers that do not accept other types of ciphers.

- **Enable Certificate Validation**: It is highly recommended to select this for the DTC server certificate to be validated by NIOS.
  - **Enable SNI (Server Name Indication)**: Specify if you want to use SNI for the health monitor to connect to a specific DTC server by hostname. In addition, you should indicate an alternate SNI hostname in the DTC server editor.

5. Click Next and complete the following:

- **HTTP Request**: Specify the HTTP request to send the query from the client to the server. The appliance displays GET/ by default. You can specify an HTTP request up to 1024 characters. For more information, see Editing HTTP Request for HTTP Health Monitor.
- **Response Code Check**: Specify in which case the response code from the server is valid:
  - Select Any response code is valid, if any response code from the server is required.
  - Select A valid response code, select equals or does not equal, and then specify a value. The default value is 200.
- **Response Content Check**: Specify an option for checking the server response content:
  - Select Do not check the response content to not perform any content check.
  - Select Search for a string in the response content to search for a string in the response content. Then do the following:
    1. In the Search in drop-down list, choose where to perform the search for a string: in Both the header or body, Body, or Headers of the HTTP request. The search is limited to the first five kilobytes of the response.
    2. In the Regular Expression field, specify a regular expression that will be used to search for a string in the response content.
    3. In the drop-down list The content is valid if the regular expression is, select either found or not found. If you select found, the content is valid if it corresponds to the regular expression you specify. If you select not found, the content is valid if it does not correspond to the regular expression you specify.
  - Select Extract content from the response and compare it to a value to extract a certain part of the content and compare it to a specific string or integer value. Then do the following:
    1. In the Search in drop-down list, choose where to perform the search for a string: in Both the header or body, Body, or Headers of the HTTP request. Note that the search is limited to the first five kilobytes.
    2. In the Regular Expression field, specify a regular expression for content extraction. The regular expression can contain subexpressions that you may specify in the next step.
    3. Select Check all extracted content to or select Check content that is extracted using the <...> subexpression and choose one of the subexpression from the drop-down list. You can choose from the first to the eighth subexpression previously defined in the Regular Expression field.
    4. In the field The extracted content is valid if it is a, select the expected data type of the extracted content, string or integer, and select a comparison operator. Then specify a value in the text field.

6. Click Next to add extensible attributes. For information, see Using Extensible Attributes.

7. To schedule the change, click Next or Schedule for Later. In the Schedule Change panel, click Now to immediately execute this task. Or, click Later to schedule this task, and then specify a date, time, and time zone.

8. Save the configuration.

Editing HTTP Request for HTTP Health Monitor

You can specify a multi-line message and include HTTP headers in the request by using the HTTP Request field in the HTTP health monitor properties. The header lines of an HTTP request have the simple name: value syntax. The request headers are used to pass cookies, authentication, and provide information about the client to the server, etc.

The HTTP 1.1 contains a request line and a single host header:

Example 1:
GET /HTTP/1.1
Host: www.yoursite.com
Connection: close

Example 2:
GET /index.html HTTP/1.1
Host: www.example.com
Note that the lines are terminated with two chars `\n`. The whole request terminates with an empty line "\n\n\n" character sequence. NIOS adds `\n\n` string if it is absent. You can request GET / instead of GET/index.html.

The host header differentiates between several HTTP servers that are running on a single IP address on the same port. In HTTP 1.1, the server keeps the connection alive by default after the response is sent. You can disable the connection by adding a Connection: close header line to the request.

An HTTP 1.0 request may consist of a single line followed by the automatically added `\n\n`:

GET /index.html HTTP/1.0

Or in the most simple form:

GET / HTTP/1.0

The server closes the connection after the response has been sent. You can use Connection: Keep-Alive header to alter this behavior. The Context-Length header is important to determine the end of the response for keep-alive connections.

Apart from HTTP 1.0/1.1, NIOS also supports a request format known as HTTP 0.9:

GET /index.html

or

GET /

Normally, the response header consists of a response line, such as HTTP/1.1 200 OK or HTTP/1.0 400 Bad Request, followed by a couple of header lines, and then by an empty line which signals the end of the response header. With HTTP 0.9, the response immediately starts with the content of the requested file, which means that there is no HTTP return code for an HTTP 0.9 request.

Testing HTTP Health Monitors

After the HTTP health monitor is configured, you can test the configuration for a specific DTC server. Note that if you make changes to the HTTP health monitor settings, you must save the configuration so you can run the test.

To test the HTTP health monitor, do the following:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab, and then click Manage Health Monitors in the Toolbar.
2. In the Health Monitors Manager, click the Action icon

   ![Icon](image)

   next to the HTTP health monitor name and select Edit.
3. Select the Request/Response tab.
4. Click Test HTTP Health Monitor.
5. In the field Select a DTC Server or enter the IP address or domain name of an HTTP server, do one of the following to specify the server to test:
   - Click Select to select an existing DTC server.
   - Enter the IP address or host name of an HTTP server. The IP address can be IPv4 or IPv6.
6. In the field Select a Grid member that is running DTC, select a DTC server on which the test will be run.
   - If there is only one DTC server with the DTC license, it is selected by default. If there are several DTC servers with the license, the Grid Master is selected by default. If there is no Grid Master with the DTC license and there are several member servers with the license, click Select and choose a server.
7. Click Test.
8. In the result of the test, the following information is returned:
   - Test status
   - Status message

Configuring ICMP Health Monitors

An ICMP monitor sends an ICMP or ICMPv6 echo request to the IP address of the target server and expects an ICMP/ICMPv6 echo response. The ICMP monitor determines the health of a server by monitoring the response to an ICMP ping.

1. From the Data Management tab, select the DNS tab -> Traffic Control tab, and then click Manage Health Monitors in the Toolbar.
2. In the Health Monitors Manager, click the arrow next to the Add icon and select ICMP Health Monitor.
3. In the ICMP Health Monitor Wizard, complete the following:
   - Name: Enter a name for the ICMP health monitor.
   - Interval (seconds): Enter the interval value in seconds. The health monitor runs only for the specified interval and it is measured from the end of the previous monitor cycle. The default value is five.
   - Timeout (seconds): Enter the timeout value in seconds. The monitor waits for the number of seconds that you specify after sending a response. If it does not receive a response within the number of seconds that you specify, then the appliance considers this check as failed. The monitor discards any response it receives after the timeout. The default value is 15.
   - Retry Up Count: Enter a retry up count. When you specify a value, the appliance checks whether the server is up based on the following: interval"retry up count". For example, if you specify the interval as five seconds and the retry up count as 10 seconds, then the appliance tries to connect to the server every five seconds for a period of 50 seconds. If the server is down initially, the appliance tries to connect to the server for 50 seconds in sequence. When the connection is successful, the ICMP monitor considers the server to be up. If the server is unavailable for an entire period of 50 seconds, the appliance considers this connection as a failure.
   - Retry Down Count: Enter a retry down count. The ICMP monitor considers the server unavailable only if the server is
unavailable during the period: \(\text{interval} \times \text{retry down count}\). For example, if you specify the interval as five seconds and the retry down count as 10 seconds, then the appliance checks if the server is unavailable for 50 seconds in sequence. If the server is unavailable for an entire period of 50 seconds, the appliance considers the server to be down.

- **Comment**: Enter information about the ICMP health monitor.

4. Click **Next** to add extensible attributes. For information, see *Using Extensible Attributes*.

5. To schedule the change, click **Next** or **Schedule for Later**. In the **Schedule Change** panel, select **Now** to immediately execute this task. Or select **Later** to schedule this task, and then specify a date, time, and time zone.

6. Save the configuration.

### Configuring PDP Health Monitors

A PDP (Packet Data Protocol) monitor sends a standard GTP ECHO request to the server. The GTP (GPRS Tunneling Protocol) echo message is used to ping the server. The connection is successful when the monitor receives an ECHO response from the server. If the server does not respond after a specified number of echo requests, the server is declared down by the monitor. You cannot modify the request or response.

1. From the **Data Management** tab, select the **DNS** tab -> **Traffic Control** tab, and then click **Manage Health Monitors** in the Toolbar.
2. In the Health Monitors Manager, click the arrow next to the Add icon and select **PDP Health Monitor**.
3. In the **PDP Health Monitor Wizard**, complete the following:
   - **Name**: Enter a name for the PDP health monitor.
   - **Interval (seconds)**: Enter the interval value in seconds. The health monitor runs only for the specified interval and it is measured from the end of the previous monitor cycle. The default value is five.
   - **Timeout (seconds)**: Enter the timeout value in seconds. The monitor waits for the number of seconds that you specify after sending a response. If it does not receive a response within the number of seconds that you specify, then the appliance considers this check as failed. The monitor discards any response it receives after the timeout. The default value is 15.
   - **Retry Up Count**: Enter a retry up count. When you specify a value, the appliance checks whether the server is up based on the following: \(\text{interval} \times \text{retry up count}\). For example, if you specify the interval as five seconds and the retry up count as 10 seconds, then the appliance tries to connect to the server for 50 seconds in sequence. If the server is up initially, the appliance considers the server to be up if the server is available for an entire period of 50 seconds.
   - **Port**: Specify a port for PDP connection. The appliance displays 2123 by default. You can specify a value between zero and 65535.
   - **Comment**: Enter information about the PDP health monitor.

4. Click **Next** to add extensible attributes. For information, see *Using Extensible Attributes*. To schedule the change, click **Next** or **Schedule for Later**. In the **Schedule Change** panel, select **Now** to immediately execute this task. Or select **Later** to schedule this task, and then specify a date, time, and time zone.

5. Save the configuration.

### Configuring SIP Health Monitors

A SIP monitor sends a standard SIP OPTIONS request to the server. You cannot modify this request. The monitor accepts only direct responses from the server and does not open alternate connections. The SIP monitor determines the health of the SIP server such as SIP proxies and session border controllers, and SIP gateways by issuing SIP OPTIONS to the server and examining the response provided by the server. The service is considered available if the response received from the server matches the expected response. The SIP monitor does not support SCTP transport. It does not receive SIP connections. Responses are normally received over the same connection as the request was sent. The server does not attempt to open a new connection to send the response when it encounters an error message.

1. From the **Data Management** tab, select the **DNS** tab -> **Traffic Control** tab, and then click **Manage Health Monitors** in the Toolbar.
2. In the Health Monitors Manager, click the arrow next to the Add icon and select **SIP Health Monitor**.
3. In the **SIP Health Monitor Wizard**, complete the following:
   - **Name**: Enter a name for the SIP health monitor.
   - **Interval (seconds)**: Enter the interval value in seconds. The health monitor runs only for the specified interval and it is measured from the end of the previous monitor cycle. The default value is five.
   - **Timeout (seconds)**: Enter the timeout value in seconds. The monitor waits for the number of seconds that you specify after sending a response. If it does not receive a response within the number of seconds that you specify, then the appliance considers this check as failed. The monitor discards any response it receives after the timeout. The default value is 15.
   - **Retry Up Count**: Enter a retry up count. When you specify a value, the appliance checks whether the server is up based on the following: \(\text{interval} \times \text{retry up count}\). For example, if you specify the interval as five seconds and the retry up count as 10 seconds, then the appliance tries to connect to the server every five seconds for a period of 50 seconds. If the server is down initially, the appliance tries to connect to the server for 50 seconds in sequence. When the connection is successful, the SIP monitor
Consider the server to be up. If the server is unavailable for an entire period of 50 seconds, the appliance considers this connection as a failure.

- **Retry Down Count**: Enter a retry down count. The SIP monitor considers the server unavailable only if the server is unavailable during the period: interval*retry down count. For example, if you specify the interval as five seconds and the retry down count as 10 seconds, then the appliance checks if the server is unavailable for 50 seconds in sequence. If the server is unavailable for an entire period of 50 seconds, the appliance considers the server to be down.
- **Comment**: Enter information about the SIP health monitor.

4. Click Next and complete the following:
   - **Expected Return Code**: The response code expected from the server. Select a value from the drop-down list: any, equals, and does not equals. When you select equals or does not equals, the appliance displays 200 by default. You can specify a value between zero and 999.
   - **Port**: Specify a port for SIP connection. The appliance displays 5060 for TCP and UDP transport by default. When you select SIPS and TLS transport options, the appliance displays 5061 by default. You can specify a value between zero and 65535.
   - **Transport**: Select a transport option from the drop-down list: SIPS, TCP, TLS, and UDP. If you select SIPS or TLS, specify any of the following related options that become available
     - **Client Certificate**: Click Certificate to select a client certificate. Select a certificate from the dialog box. Click Clear to delete the certificate that you have uploaded. The monitor does not inspect or validate the server certificate, if any. For information about how to upload certificates, see Managing Health Monitor Certificates.
   - **Ciphers**: Specify a list of SSL ciphers in an OpenSSL format. You can specify text up to 1024 character.

The following example commands list some available ciphers:

**Example 1:**
```
openssl ciphers 'HIGH:!DES'
```

DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:
DHE-DSS-CAMELLIA256-SHA:AEAD-AES128-SHA:ADH-AES256-SHA:
CAMELLIA256-SHA:PSK-AES256-CBC-SHA:PSK-AES256-SHA:
PSK-3DES-CBC-SHA:PSK-3DES-CBC-SHA:PSK-AES128-CBC-SHA:
PSK-AES256-CBC-SHA:
```

**Example 2:**
```
openssl ciphers 'DEFAULT:!EDH+RSA'
```

DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:
CAMELLIA256-SHA:PSK-AES256-CBC-SHA:PSK-3DES-EDE-CBC-SHA:
PSK-3DES-CBC-SHA:PSK-3DES-EDE-CBC-SHA:
HMAC-SHA256:
```

Note: The DHE cipher list family ("Diffie-Hellman key agreement" plus "RSA authentication") could consume excessive CPU and is excluded from the defaults used by DNS Traffic Control health monitors. Although you can enable these ciphers by explicitly configuring them in the cipher list for HTTPS and SIP monitors, you should be aware that doing so will increase CPU usage. Since health monitoring in general does not require high security, Infoblox recommends that you enable these ciphers only for target servers that do not accept other types of ciphers.

- **Enable Certificate Validation**: It is highly recommended to select this for the DTC server certificate to be validated by NIOS.

5. Click Next to add extensible attributes. For information, see Using Extensible Attributes.

6. To schedule the change, click Next or Schedule for Later. In the Schedule Change panel, select Now to immediately execute this task. Or select Later to schedule this task, and then specify a date, time, and time zone.

7. Save the configuration.

### Configuring SNMP Health Monitors

An SNMP health monitor sends an SNMPv1, SNMPv2c, or SNMPv3 request to the monitored server. The SNMP agent in the managed server provides the data in the form of variables, and each variable is associated with an unique OID (object identifier). An OID is a dotted-decimal number that defines the location of the object in the universal MIB tree. You can manually enter up to 15 OIDs to be monitored by the SNMP monitor. The server is considered available if the response received from the server matches the expected result for all OIDs. If the server does not respond after a specified number of requests, the server is declared down by the monitor.

To configure an SNMP OID health monitor, complete the following:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab, and then click Manage Health Monitors in the Toolbar.
2. In the Health Monitors Manager, click the arrow next to the Add icon and select SNMP Health Monitor.
3. In the SNMP Health Monitor Wizard, complete the following:
   - **Name**: Enter a name for the SNMP monitor.
   - **Interval (seconds)**: Enter the interval value in seconds. The health monitor runs only for the specified interval and it is measured
from the end of the previous monitor cycle. The default value is five.

- **Timeout (seconds):** Enter the timeout value in seconds. The monitor waits for the number of seconds that you specify after sending a response. If it does not receive a response within the number of seconds that you specify, then the appliance considers this check failed. The monitor discards any responses it receives after the timeout. The default value is fifteen.

- **Retry Up Count:** Enter a retry up count. When you specify a value, the appliance checks whether the server is up based on the following: interval*retry up count For example, if you specify the interval as five seconds and the retry up count as 10, then the appliance tries to connect to the server every five seconds for a period of 50 seconds. If the server is down initially, the appliance tries to connect to the server for 50 seconds in sequence. When the connection is successful, the SNMP monitor considers the server to be up. If the server is unavailable for an entire period of 50 seconds, the appliance considers this connection as a failure.

- **Retry Down Count:** Enter a retry down count. The SNMP monitor considers the server unavailable only if the server is unavailable during the period: interval*retry down count For example, if you specify the interval as five seconds and the retry down count as 10, then the appliance checks if the server is unavailable for 50 seconds in sequence. If the server is unavailable for an entire period of 50 seconds, the appliance considers the server to be down.

- **Port:** Specify a port for the SNMP connection. The appliance displays 161 by default. You can specify a value between zero and 65535.

- **Comment:** Enter information about the SNMP health monitor.

4. Click **Next** and complete the following:

- **Version:** Select the SNMP version, **v1**, **v2c**, or **v3**. Note that the available options for versions v1 and v2c differ from those for v3 version.

- **(SNMPv1 and SNMPv2c only) Community:** Enter the text string that the SNMP monitor must send along with the queries to the server for authentication. The community string is similar to a password and the server accepts queries only from the SNMP monitor that provide the correct community string. Note that this community string must match exactly what you enter in the management system. The default value is **public**.

- **(SNMPv3 only) SNMPv3User:** Click **Select** or **Create** to specify an SNMPv3 user. For information about SNMPv3 users, see Configuring SNMPv3 Users.

If you are modifying an already existing SNMPv3 health monitor in the SNMP Health Monitor editor, two additional optional fields become available:

- **Context:** enter an arbitrary string.
- **EngineID:** enter an arbitrary string that can contain from 10 to 64 hexadecimal digits (5 to 32 octet numbers).

Click the Add icon above the Health Monitor SNMP OIDs table to add an SNMP OID entry. Complete the following:

- **OID:** Specify the object identifier. An OID is a unique dotted-decimal number that identifies the location of the object in the MIB tree. For more information about OIDs, see SNMP MIB Hierarchy.

- **Type:** Select either **String** or **Integer** from the drop-down list.

**Note:** If you use this SNMP monitor with the Ratio: Dynamic load balancing method, note that only integer OID type is supported for this method.

- **Operator:** Select one of these operators from the drop-down list: **Any**, **Equals**, **Larger or equals**, **Range**, and **Smaller or equals**.

- **Value:** If the operator is **Equals**, **Larger or equals**, or **Smaller or equals**, enter a value. If the operator is **Range**, enter the minimum and maximum values in the **Min value** and **Max value** fields respectively.

- **Comment:** Enter information about the SNMP OID entry.

- **Click Add** to add the SNMP OID to the table.

5. Click **Next** to add extensible attributes. For information, see Using Extensible Attributes.

6. To schedule the change, click **Next** or **Schedule for Later**. In the Schedule Change panel, select **Now** to immediately execute this task. Or select **Later** to schedule this task, and then specify a date, time, and time zone.

7. Save the configuration.

### Configuring TCP Health Monitors

A TCP monitor opens a TCP connection to communicate between the appliance and server. The connection is successful only when the handshake is complete. A successfully opened connection will be immediately closed or reset.

1. From the **Data Management** tab, select the **DNS** tab -> **Traffic Control** tab, and then click Manage Health Monitors in the Toolbar.
2. In the Health Monitors Manager, click the arrow next to the Add icon and select TCP Health Monitor.
3. In the **TCP Health Monitor Wizard**, complete the following:

   - **Name:** Enter a name for the TCP health monitor.
   - **Interval (seconds):** Enter the interval value in seconds. The health monitor runs only for the specified interval and it is measured from the end of the previous monitor cycle. The default value is five.
   - **Timeout (seconds):** Enter the timeout value in seconds. The monitor waits for the number of seconds that you specify after sending a response. If it does not receive a response within the number of seconds that you specify, then the appliance considers this check as failed. The monitor discards any response it receives after the timeout. The default value is fifteen.
   - **Retry Up Count:** Enter a retry up count. When you specify a value, the appliance checks whether the server is up based on the following: interval*retry up count. For example, if you specify the interval as five seconds and the retry up count as 10 seconds, then the appliance tries to connect to the server every five seconds for a period of 50 seconds. If the server is down initially, the
appliance tries to connect to the server for 50 seconds in sequence. When the connection is successful, the TCP monitor considers the server to be up. If the server is unavailable for an entire period of 50 seconds, the appliance considers this connection as a failure.

- **Retry Down Count**: Enter a retry down count. The TCP monitor considers the server unavailable only if the server is unavailable during the period: interval*retry down count. For example, if you specify the interval as five seconds and the retry down count as 10 seconds, then the appliance checks if the server is unavailable for 50 seconds in sequence. If the server is unavailable for an entire period of 50 seconds, the appliance considers the server to be down.
- **Port**: Specify a port for TCP connection. You can specify a value between zero and 65535.
- **Comment**: Enter information about the TCP health monitor.

4. Click **Next** to add extensible attributes. For information, see Using Extensible Attributes.
5. To schedule the change, click **Next** or **Schedule for Later**. In the Schedule Change panel, select **Now** to immediately execute this task. Or select **Later** to schedule this task, and then specify a date, time, and time zone.
6. Save the configuration.

Managing Health Monitor Certificates

You can upload multiple certificates to the appliance and associate them with HTTP and SIP health monitors. The appliance supports certificates that are in PEM or PKCS#12 format only. A PEM file can contain more than one certificate. Note that the uploaded certificate must include both the client certificate and the private key. You can add, delete or view certificates.

To upload a health monitor certificate:

1. From the **Data Management** tab, select the **DNS** tab -> **Traffic Control** tab, and then click **Manage Health Monitors** in the Toolbar.
2. In the Health Monitors Manager, click the Manage Health Monitor Certificates icon.
3. In the **Health Monitor Certificates** window, click the Add icon.
4. In the **Upload** window, click **Select** and navigate to the certificate you want to upload.
5. Select the file and click **Upload**.

Grid Manager displays the following information in the **Health Monitor Certificates** window:

- **Issuer**: The name of the trusted CA that issued the certificate.
- **Valid From**: The date from which the certificate becomes valid.
- **Valid To**: The date until which the certificate is valid.
- **Subject**: The name of the certificate.

To upload a certificate from a web browser:

1. Export a PEM file from a web browser.
2. Generate a private key using the following command:

   ```
   openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout mycert.pem -out mycert.pem
   ```
3. Copy the private key section out of mycert.pem and add it to the PEM file from the web browser.
4. Or add both the PEM and the private key together as PKCS#12.

You can also do the following in the **Health Monitor Certificates** window:

- Click the check box next to the issuer and click the Delete icon to delete it.
- Print the data or export it in .csv format.

Modifying Health Monitors

To modify a health monitor:

1. From the **Data Management** tab, select the **DNS** tab -> **Traffic Control** tab, and then click **Manage Health Monitors** in the Toolbar.
2. In the Health Monitors Manager, click the **Action** icon next to the health monitor name, and select **Edit** from the menu.
3. The **Health Monitor** editor contains the following tabs from which you can modify data:

   - **General**: This tab displays the health monitor **Name**, **Comment**, **Interval**, **Timeout**, **Retry Up Count**, and **Retry Down Count** fields. You can edit the values.
   - **(HTTP, SIP, and SNMP health monitors) Protocol**: This tab displays the protocol data that you can modify.
   - **(HTTP/S health monitors only) Request/Response**: This tab displays HTTP request and response check options for HTTP/S health monitors.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with the pool. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.

For information about modifying the details of specific monitors, see the corresponding sections above.

4. To schedule this task, click the Schedule icon at the top of the wizard. In the **Schedule Change** panel, select **Later** and enter a date, time, and time zone. The Schedule icon is green when there is a pending scheduled task. For information, see Scheduling Tasks.
Viewing Health Monitors

You can view health monitors that you have created. You can add new health monitors, delete existing monitors, modify health monitors, or associate extensible attributes to them. You can also upload and manage health monitor certificates.

To view health monitors:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab, and then click Manage Health Monitors in the Toolbar.
2. The Health Monitors Manager displays the following information:
   - **Name**: The name of the health monitor.
   - **Type**: The type of health monitor.
   - **Comment**: Displays information about the health monitor.
   - **Interval**: The interval value in seconds.
   - **Timeout**: The timeout value in seconds.
   - **Retry Up Count**: The retry up count specified for the respective health monitor.
   - **Retry Down Count**: The retry down count specified for the respective health monitor.
   - **Port**: The port number specified for the respective health monitor. Note that this is not valid for an ICMP monitor.
   - **Site**: Value that was entered for the respective health monitor.

   You can do the following in the Health Monitors Manager:
   - Define new health monitors. For more information, see the following sections:
     - Configuring HTTP Health Monitors
     - Configuring ICMP Health Monitors
     - Configuring PDP Health Monitors
     - Configuring SIP Health Monitors
     - Configuring SNMP Health Monitors
     - Configuring TCP Health Monitors
   - Edit existing health monitors. For more information, see Modifying Health Monitors.
   - Manage health monitor certificates. For more information, see Managing Health Monitor Certificates.
   - Delete existing health monitors. For more information, see Deleting Health Monitors.
   - Click the Export icon to export the list of monitors to a .csv file.
   - Click the Print icon to print the list of monitors.
   - Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the monitor from the possible matches. Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.

Deleting Health Monitors

To delete a health monitor:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab, and then click Manage Health Monitors in the Toolbar.
2. In the Health Monitors Manager, click the Action icon next to the health monitor name and select Delete from the menu.
3. In the Delete Confirmation dialog box, click Yes to delete or No to cancel.

   Click Schedule Deletion and in the Schedule Change panel, enter a date, time, and time zone to schedule deletion at a later date and time. For more information, see Scheduling Deletions.

Managing DNS Traffic Control Objects

You can configure DNS Traffic Control servers, pools, and LBDNs on the NIOS appliance. You can define multiple servers, pools, or LBDNs.

Configuring DNS Traffic Control Servers

DNS Traffic Control servers are objects that are associated with synthesized A, AAAA or CNAME records. DNS Traffic Control servers can be in multiple pools and can be the destination for multiple topology rulesets. You can disable a server while in use, but note that this affects the pools that are associated with the server. You cannot disable a server if it is the last active server for any pool with which it is associated. To disable such a server, first remove it from the associated pools and topology rulesets.

You can add a DTC server on the Traffic Control tab. Alternatively, you can do this on the DNS -> Zones tab or Members/Servers tab by selecting an existing A, AAAA, or host record in the table and clicking Create DTC Server in the Toolbar or in the record's action menu.

You can also add a DTC server on the Data Management -> IPAM tab based on a selected existing A or host record. You can do so on both IP Map and List subtabs.

If you use multi-tier architecture and want to monitor the availability of separate components of the DTC server, you can add a health monitor for
To configure a DTC server, complete the following:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab.
2. In the Toolbar, click the arrow next to the Add icon and select Server.
3. In the DTC Server Wizard, under Select an existing DNS record or enter the Name and Host fields, do one the following:
   - Optionally, click Select and choose an existing DNS record which will pre-populate the server information:
     a. Select a zone using the filter and click Apply.
     b. Select the record type, Host, A, or AAAA, by which to filter the records list.
     c. Click the required record name to select it.
   - Specify the DTC server name and host:
     - Name: Enter the name of the DTC server.
     - Host: Specify the server host by selecting and specifying one of the following:
       - IP Address: The DTC response from the server will contain an auto-created A (IPv4) or AAAA (IPv6) record with this IP address.
       - Domain Name: The DTC response from the server will contain an auto-created CNAME record that uses this domain name.

Note: This step only applies if you create a DTC server from the Traffic Control tab. If you create a DTC server on the DNS -> Zones, DNS -> Members/Servers tab, or Data Management -> IPAM tab, the record is already selected so this step is not available in the DTC Server Wizard.

4. Auto-create DTC records: If this is enabled and the Host field contains an IP address, an A (IPv4) or AAAA (IPv6) record will be created. If the Host field contains a domain name, a CNAME record will be created. If you do not enable auto-created DTC records, you must create those records manually. For more information, see 4820176

Note: A record type that corresponds to the Host field must exist in order for the DTC Server to return a response.

5. Comment: Enter additional information about the server.
6. Disabled: Select this to disable the server.
7. Click Next to define extensible attributes. For information, see Using Extensible Attributes.
8. To schedule the change, click Next or Schedule for Later. In the Schedule Change panel, select Now to immediately execute this task. Or select Later to schedule this task, and then specify a date, time, and time zone.
9. Save the configuration.

Managing DTC Server Records

You can create A, AAAA, CNAME, and NAPTR records in a DTC server similar to the NAPTR record in a DNS zone.
A NAPTR (Name Authority Pointer) record specifies a rule that uses a substitution expression to rewrite a string into a domain name or URI (Uniform Resource Identifier). A URI is either a URL (Uniform Resource Locator) or URN (Uniform Resource Name) that identifies a resource on the Internet. For information about NAPTR records, see Managing NAPTR Records.

You can assign multiple A, AAAA, and NAPTR records simultaneously to a DTC server or only one CNAME record. Enabled CNAME record cannot coexist with enabled A, AAAA, or NAPTR record. Disabled CNAME record cannot coexist with enabled CNAME record.
This section describes how to add, modify, and delete records in a DTC server. It includes the following sections:

- 4820176
- 4820176
- 4820176
- 4820176

Adding DTC Records

To add a DTC record:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab -> DTC server -> click Add -> A Record/AAAA Record/CNAME Record/NAPTR Record.
2. Enter the information in the Add DTC Record wizard.
   - For an A record:
     - IP address: Enter an IPv4 address for the A record on the DTC server.
     - Comment: Optionally, enter additional information about the A record.
     - Disable: Select this check box to disable the record. Clear the check box to enable it.
   - For an AAAA record:
     - IP address: Enter an IPv6 address for the AAAA record on the DTC server.
     - Comment: Optionally, enter additional information about the AAAA record.
• Disable: Select this check box to disable the record. Clear the check box to enable it.

• For a CNAME record:
  • Canonical name: Enter the complete canonical (or official) name of the host.
  • Comment: Optionally, enter additional information about the CNAME record.
  • Disable: Select this check box to disable the record. Clear the check box to enable it.

• For a NAPTR record:
  • Service: Specifies the service and protocol used to reach the domain name that results from applying the regular expression or replacement. You can enter a service or select a service from the list.
  • Flags: The flag indicates whether the resulting domain name is the endpoint URI or if it points to another record. Select one of the following:
    • U: Indicates that the output maps to a URI.
    • S: Indicates that the resulting domain name has at least one SRV record.
    • A: Indicates that the resulting domain name has at least one A or AAAA record.
    • P: Indicates that this record contains information specific to another application.

  Leave this blank to indicate that the DNS client must use the resulting domain name to look up other NAPTR records. You can use the NAPTR records as a series of rules that are used to construct a URI or domain name.

  • Order: Select an Integer from 10 to 100, or enter a value from 0 to 65535. This value indicates the order in which the NAPTR records must be processed. The record with the lowest value is processed first.
  • Preference: Select an Integer from 10 to 100, or enter a value from 0 to 65535. Similar to the Preference field in MX records, this value indicates which NAPTR record should be processed first when the records have the same Order value. The record with the lowest value is processed first.
  • REGEX: The regular expression that is used to rewrite the original string from the client into a domain name. RFC 2915 specifies the syntax of the regular expression. Note that the appliance validates the regular expression syntax between the first and second delimiter against the Python re module, which is not 100% compatible with POSIX Extended Regular Expression as specified in the RFC. For information about the Python re module, refer to http://docs.python.org/release/2.5.1/lib/module-re.html.
  • Replacement: This specifies the domain name for the next lookup. The default is a dot (.), which indicates that the regular expression in the REGEX field provides the replacement value. Alternatively, you can enter the replacement value in FQDN format.
  • Comment: Optionally, enter a descriptive comment for this record.
  • Disable: Clear the check box to enable the record. Select the check box to disable it.

3. To schedule the change, click Next or Schedule for Later. In the Schedule Change panel, select Now to immediately execute this task. Or select Later to schedule this task, and then specify a date, time, and time zone.

4. Save the configuration and click Restart if it appears at the top of the screen.

**Viewing DTC Records**

To view the records associated with a DTC server, go to the Data Management tab, select the DNS tab -> Traffic Control tab -> DTC server. The Grid Manager displays the following for each DTC record:

• Type: The type of record.
• Data: The data that the record contains. For a NAPTR record, this field displays the following data: Order, Preference, Flags, Services, REGEX, and Replacement.
• Comment: Comment that was entered for the record.
• TTL: The TTL (time-to-live) value of the record.
• Disabled: Indicates if the record is disabled.

You can do the following:

• Click the Add icon to add a DTC record.
• Select a record and click the Edit icon to edit the configuration. You can also click the Action icon next to the record and select Edit from the menu.
• Select a record and click the Delete icon to delete it. You can also click the Action icon next to the record and select Delete from the menu.
• Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
• Click the Export icon to export the list of DTC records to a .csv file.
• Click the Print icon to print the list of DTC records.

**Modifying DTC Records**

To modify a DTC record:
1. From the **Data Management** tab, select the **DNS** tab -> **Traffic Control** tab -> **DTC server**.

2. Select the DTC record you want to modify, and click the **Edit** icon.

3. The **DTC Record** editor contains the following tabs from which you can modify information:
   - **General**: You can modify most of the information, except for the read-only fields, such as the DNS view. For a description of the fields, see 4820176
   - **TTL**: You can modify the TTL setting. For information, see **About Time To Live Settings**.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Deleting DTC Records

To delete a DTC record:

1. From the **Data Management** tab, select the **DNS** tab -> **Traffic Control** tab -> **DTC server**.

2. Select the DTC record you want to delete, and click the **Delete** icon.

3. When the confirmation dialog box displays, select **Yes**.

Grid Manager moves the DTC record to the Recycle Bin, from which you can restore or permanently delete the record. For information, see Using the Recycle Bin.

### Modifying DNS Traffic Control Servers

To modify a DNS Traffic Control server:

1. From the **Data Management** tab, select the **DNS** tab -> **Traffic Control** tab, click the **Edit** icon next to the DTC server and select **Edit** from the menu.

2. The **DTC Server** editor contains the following tabs from which you can modify data.
   - **General**: This tab displays the **Name**, **Host**, **Auto-create DTC records**, and **Comment** that you entered while configuring the server. You can enable or disable the server. For information about how to modify the server data, see 4820176 Additionally, specify the Server Name Indication setting:
     - **UseAlternateSNIHostname**: If the SNI name is different from what is configured in the address field, select this check box and enter the required hostname by which an HTTPS health monitor should connect to the server.
   - **Health Monitors**: Define health monitors for the DTC server:
     1. In **Health Monitor**, select the monitor type: icmp, http, https, sip, pdp, or snmp.
     2. In **Domain Name or IP Address**, type either the FQDN or the IP address to monitor.
     3. In **If required, add more health monitors for the server as described above. You can add up to ten health monitors per server.**
     4. In **Health Monitors from Pools**, you can see other health monitors assigned to the pools that the server belongs to. The availability requirement for the pools must be set to either "All" or "Any" for you to be able to add server-specific health monitors. For information, see Configuring DNS Traffic Control Pools.

3. To schedule this task, click the **Schedule** icon at the top of the wizard. In the **Schedule Change** panel, select **Later** and enter a date, time, and time zone. The Schedule icon is green when there is a pending scheduled task. For information, see Scheduling Tasks.

4. Save the configuration.

### Configuring DNS Traffic Control Pools

A pool contains load balanced servers. You can define multiple servers for a pool. Each LBDN must have at least one pool associated with it to be operational. For sites with a large amount of incoming traffic, you can configure DNS Traffic Control to distribute client requests to multiple servers using a load balancing pool. An individual server can belong to one or more load balancing pools, depending on how you want to manage your network traffic. You can also set the order of servers in the pool and define a ratio on a server basis.

A pool can contain preferred and alternative load balancing methods. You can define permissions on these pools and associate extensible attributes with them. Each pool can contain one or more health monitors associated with it. You can define TTLs at the LBDN level. These TTLs are valid for dynamic RRsets that are created by the querying process for each query.

To configure a pool:

1. From the **Data Management** tab, select the **DNS** tab -> **Traffic Control** tab, and then click the arrow next to the **Add** icon and select **Pool**.

2. In the **DTC Pool Wizard**, complete the following:
   - **Name**: Enter the name of the pool.
• **Comment**: Enter additional information about the pool.
• **Disabled**: Select this to disable the pool.

3. Click **Next** to associate health monitors with the pool:

   • **Health Monitors**: Select the health monitor from the **Available** table, which you want to associate with the pool, and click the right arrow to move the selected health monitor to the **Active** table. You can use SHIFT+click and CTRL+click to select multiple health monitors. To dissociate the health monitor from the pool, select it and click the left arrow to move it to the **Available** pane from the **Active** pane.

   • **Availability Requirements**: Select from the following:
     - **All**: All active monitors must report the available status for the pool to be determined as available.
     - **Any**: Any number of active monitors must report the available status for the pool to be determined as available.
     - **At least**: The minimum number of active monitors that must report the available status for the pool to be determined as available.

4. Click **Next** and select the preferred load balancing method:

   • **All Available**
   • **Ratio**: Dynamic (see details below in the procedure)
   • **Global Availability**
   • **Ratio**: Fixed
   • **Round Robin**
   • **Topology** (see details below in the procedure)

   For more information, see [Load Balancing Methods for DNS Traffic Control](#).

5. If you select **Ratio**: Dynamic as preferred method, also select a dynamic ratio method from the following:

   • **Round Trip Delay**: Select this to enable load balancing based on the proximity of DTC servers determined through round trip delay. Specify the following:
     - **Monitor**: Select a pre-configured health monitor to use for monitoring the round trip delay.
   • **SNMP**: Select this to enable load balancing based on a server metric captured by an SNMP health monitor. Specify the following:
     - **Monitor**: Select a health monitor for which to track a server metric.
     - **OID**: Specify an object identifier that indicates the metric to track.
     - **Weighing**: Select to weigh DTC servers by priority or ratio.
     - **Inverse OID value**: Select this if you want to use the value of the monitored metric as inversed for convenience of determining servers availability.

6. If you select **Topology** as preferred method, also select a Topology Ruleset. Only topology rulesets with the Server destination type are displayed in the drop-down list.

   **NOTE**: If you select Topology as the preferred method, you can also specify the alternate method which is used to select a server from the pool if the preferred one does not return any result. The preferred and alternate methods must be different.

7. If applicable, select the alternate load balancing method.

   • **All Available**
   • **Ratio**: Dynamic
   • **Global Availability**
   • **None**
   • **Ratio**: Fixed
   • **Round Robin**
   • **Topology**

   For details on each alternate method, see the description of the preferred method above.

8. Click **Next** to associate servers with the pool. Click the Add icon, select a server from the **DTC Server Selector** dialog box and click **OK**. You can use SHIFT+click and CTRL+click to associate multiple servers. The appliance displays the following information:

   • **Server Name**: The name of the DNS Traffic Control server.
   • **Host**: The host address of the server.
   • **Ratio**: You can modify the ratio value. The value must be greater than zero.
   • **Disabled**: Indicates whether the server is disabled.
   • **Order**: Displays the order of servers in the list.

   To dissociate a server from the pool, select the check box next to the server name and click the Delete icon.

9. Click **Next** to define extensible attributes. For information, see [Using Extensible Attributes](#).

10. To schedule the change, click **Next** or **Schedule for Later**. In the **Schedule Change** panel, select **Now** to immediately execute this task. Or select **Later** to schedule this task, and then specify a date, time, and time zone.

11. Save the configuration.
Modifying DNS Traffic Control Pools

To modify a pool:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab, click the Action icon next to the pool name and select Edit from the menu.

2. The DTC Pool editor contains the following basic tabs from which you can modify data. For information about how to modify data, see 4820176

   - **General**: This tab displays the pool Name and Comment. You can edit the values and enable or disable the pool.
   - **TTL**: This tab displays the TTL value configured for the pool. The default value is inherited from the LBDNs which are using the pool. There can be multiple inheritance. Click Override to override the value.
   - **Health Monitors**: This tab displays health monitors that are associated with the pool. You can associate new health monitors or dissociate the health monitors that are already associated with the pool.
   - **Load Balancing**: This tab displays the load balancing methods that you have selected while configuring the pool. You can select a new preferred and alternate load balancing methods.
   - **Pool Members**: This tab displays the servers that are associated with the pool. You can add new servers or delete servers that are associated with the pool. You can also modify servers ratio and order.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with the pool. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.

3. To schedule this task, click the Schedule icon at the top of the wizard. In the Schedule Change panel, select Later and enter a date, time, and time zone. The Schedule icon is green when there is a pending scheduled task. For information, see Scheduling Tasks.

4. Save the configuration.

Configuring DNS Traffic Control LBDNs

A DTC LBDN is a load balanced domain name object that is used by DNS Traffic Control to process DNS queries for load balanced resources. You can define multiple LBDNs on the NIOS appliance and associate extensible attributes to them. You can configure permissions for DTC LBDNs. For more information, see License Requirements and Admin Permissions. You can configure a load balancing method for each LBDN. You can assign multiple pools and a single load balancing method to an LBDN. You can associate or dissociate LBDNs with a zone. Note that zone transfers and incremental zone transfers ignore LBDNs. When you configure or modify DTC LBDNs, a service restart is required in order for the new configuration to take effect. On the appliance, the DNS Traffic Control querying process generates A, AAAA, NAPTR, CNAME records for an LBDN, called LBDN records. LBDN records are served by DNS Traffic Control servers. An LBDN record must be associated with an authoritative zone. For more information about LBDN records, see 4820176.

To configure an LBDN, complete the following:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab, click the arrow next to the Add icon, and select LBDN. or From the Data Management tab -> DNS tab -> Zones tab -> authoritative_zone -> Records tab, click the Add icon, and select Record -> DTC LBDN.

2. In the DTCLBDN wizard, complete the following:

   - **Display Name**: Enter a display name for the LBDN.
   - **Patterns**: Click the Add icon to add an LBDN pattern. For more information, see 4820176. To delete an LBDN pattern, select the check box next to the pattern and click the Delete icon.
   - **Load Balancing Method**: From the drop-down list, select the method you want to use for load balancing. You can select one of the following: Global Availability, Ratio:Fixed, Round Robin, and Topology. The default is Round Robin. For more information about the load balancing methods, see Load Balancing Methods for DNS Traffic Control.
     - **Topology Ruleset**: This is displayed only when you select the Topology load balancing method. In the drop-down list, only the topology rulesets with the Pool destination type are displayed. Select a topology ruleset for the Topology load balancing method. For more information, see Defining Topology Rulesets.
   - **Persistence**: Select this check box and enter a value greater than zero seconds to enable persistence for the LBDN. You can specify a period between one second to 30 minutes. If you specify zero, the appliance does not cache the requests. When you enable persistence for an LBDN, the appliance stores the results for specific LBDN responses in the DNS Traffic Control cache. When a request originates from the respective FQDN or an IP address within the specified period, the DNS server directs the request to the same server.

Note: When the persistence enabled, cached results are not guaranteed to persist for the configured duration. The maximum size of the persistence cache is limited globally by the platform. When the limit exceeds the maximum size, the oldest results are deleted. The appliance might discard persistence results if the relevant configuration changes. The appliance might reset persistence cache on an HA failover. **Priority**: Select a priority value, 1 (High), 2 (Normal), or 3 (Low). The priority value is used when there are LBDNs that have patterns matching the same FQDN and that are assigned to the same zone. In this case, the matching LBDN with the highest
priority is used. For example, an LBDN with "*.foo.com" and an LBDN with "www.*.com" patterns can be linked to the same zone "foo.com" if the LBDN with the "*.foo.com" pattern has priority 1 and the LBDN with the "www.*.com" pattern has priority 2 or 3. If there are no matches, the default LBDN is used.

- **Comment**: Enter additional information about the LBDN object.
- **Disabled**: Select this to disable the LBDN.

3. Click **Next** and complete the following:

- **Return these record types for the associated zones**: Select any or all of the following LBDN record types: A, AAAA, NAPTR, SVR and CNAME. You must select at least one record type for the LBDN, otherwise the LBDN is disabled. The patterns and the record types can overlap with another LBDN that is linked to the same zone only if their priorities differ.
  
  If you select the A or AAAA record type, the LBDN returns the corresponding record and/or a CNAME record when the client queries for any record type and if the server selected by DTC has the required data.

  However, if the client queries for CNAME explicitly, ensure that you select the CNAME record type check box for the CNAME records to be returned.

**Note**: If you select the CNAME or NAPTR record type, the LBDN returns the CNAME or NAPTR record respectively when the client queries for those records and if the server selected by DTC has the required data. As the CNAME response must be unique, the CNAME record type is unavailable for an LBDN if any pool in that LBDN uses the All Available load balancing method.

4. Click **Next** and click the Add icon to associate pools with the LBDN. Select a pool from the **DTC Pool Selector** dialog box and click **OK**. The appliance displays the following information:

- **Name**: The name of the selected pool.
- **Ratio**: The ratio of the associated server. You can edit this value.
- **Comment**: Displays information that you specified for the pool.
- **Members**: Displays the member associated with the pool.
- **Order**: Displays the order of the pools.

To dissociate a pool associated with an LBDN, select the check box next to the respective pool name and click the Delete icon.

5. Click **Next** to define extensible attributes. For information, see Using Extensible Attributes.

6. To schedule the change, click **Next** or **Schedule for Later**. In the **Schedule Change** panel, select **Now** to immediately execute this task. Or select **Later** to schedule this task, and then specify a date, time, and time zone.

7. Save the configuration and click **Restart** if it appears at the top of the screen.

### Configuring LBDN Patterns

An LBDN pattern is a domain name. You can define a pattern with multiple * and ? in any position of the domain name. Note the following about * and ?:

- A sequence of "s has the same effect as a single ".
- A sequence of ?s will match exactly as many octets as there are ?s.
- A " terminates on label boundaries and will not match a label separator. For example, "." matches foo.com but not www.foo.com.
- A ? does not match a label separator.
- An empty LBDN pattern will match the root and it is automatically changed to "." when you save the LBDN.
- An LBDN pattern matches an FQDN if the entire FQDN matches.
- LBDN patterns may contain special characters. For example, a\032 b.com contains two adjacent spaces.
- LBDN patterns do not support IDN and they will not convert Unicode to punycode. You can enter punycode, but note that the LBDN pattern matching does not support punycode.

### Managing LBDN Records

In order to manage an LBDN in an authoritative zone, you must enable the authoritative zone and associate it with the LBDN. If an LBDN pattern matches a zone name, the records of type "DTC LBDN Record" are created in that zone as proxies for the LBDN.

To view DTC LBDN records:

- Select the **Data Management** tab -> **DNS** tab -> **Zones** tab -> **authoritative_zone** -> **Records** tab.

The record name is the zone-relative portion of the pattern, including wildcards. For example, when you link an LBDN with patterns "www.*.com", "*.*.com", and "www.*.net", the following DTC LBDN records are created in the zone:

```
.name        ttl  type            data
---         ----  ----            ----
www.*.com   3600  A               192.168.1.1
www.*.com   3600  AAAA             192.168.1.1
*.com       3600  CNAME            www.*.com
*.com       3600  CNAME            www.*.net
*.*.com     3600  NAPTR            192.168.1.1
*.*.com     3600  NAPTR            192.168.1.2
*.*.com     3600  NAPTR            192.168.1.3
```

The record name can also be "*.*.com", "*.com", or even "*.*.net".
"www.a\*z\).*com", "\*\.*com", "bar\.*\.*net" to zone "foo.com", the appliance creates three LBDN records with names "" (zone origin), "www", and "www.a\*z" in the zone. These records will refer to their respective LBDN.

You cannot modify LBDN records. The appliance creates or deletes LBDN records based on the matched LBDN patterns. When you delete an LBDN, the appliance automatically deletes linked zones associated with it and deletes all LBDN records. You can edit the pattern that is associated with the respective LBDN record. For more information, see 4820176.

Note that an LBDN record is a separate object from the LBDN and each of these have separate permissions. For more information, see License Requirements and Admin Permissions.

Associating LBDNs with DNSSEC Signed Zones

If a zone is DNSSEC signed, you can still associate an LBDN, but some restrictions apply. You can set either Signed or Unsigned mode for the response from DNSSEC signed zones.

The following restrictions apply in the Signed mode:

- You cannot assign an LBDN to a zone or unassign an LBDN from a zone while signing, i.e. key rollover, is in progress for that zone. For information about key rollovers, see About Key Rollovers.
- If an LBDN is assigned to a zone for which signing is in progress, then all changes to that LBDN and its dependent configuration (including pools, servers, and topologies) are prohibited until signing completes. The only thing you can do while signing is in progress is to assign an LBDN already assigned to a signed zone to another unsigned zone.
- An LBDN assigned to a signed zone cannot use the All Available load balancing method or have a pattern with a wildcard in the zone.

Also, you cannot sign an unsigned zone with such an LBDN assigned.

In the Unsigned mode, unsigned responses in signed zones are returned. For more information about how to set the Signed or Unsigned mode, see Configuring Grid DNS Traffic Control Properties.

Note: You cannot assign any signed zone during staged Grid upgrade if not all of the NIOS appliances have been moved to a new software version. This restriction is working in both Signed and Unsigned modes.

Modifying DNS Traffic Control LBDNs

To modify an LBDN:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab, click the Action icon next to the LBDN name and select Edit from the menu.
2. The DTC LBDN editor contains the following tabs from which you can modify data. For information about how to modify data, see 4820176
   - General: This tab displays the Display Name, Patterns, Load Balancing Method, Persistence, Priority, and Comment of the LBDN object. Here you can also disable the LBDN.
   - Associated Zones and Records: This tab displays the record types that can be returned for the associated zones, the TTL, and the Associated Zones. You can select any or all of the following record types: A, AAAA, and NAPTR. Note that the default TTL value is 8 hours and is inherited from the associated zones of the Infoblox Grid. You can override this value or associate new zones with the LBDN to inherit a new value.
   - Pools: This tab displays the pools that are associated with the LBDN. You can delete an existing pool or add new pools.
   - Extensible Attributes: Add and delete extensible attributes that are associated with the LBDN. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.
3. To schedule this task, click the Schedule icon at the top of the wizard. In the Schedule Change panel, select Later and enter a date, time, and time zone. The Schedule icon is green when there is a pending scheduled task. For information, see Scheduling Tasks.
4. Save the configuration and click Restart if it appears at the top of the screen.

Testing DNS Traffic Control LBDNs

You can select an LBDN and test the DTC response for the respective LBDN. To test an LBDN, complete the following:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab.
2. In the Traffic Control panel, select the LBDN object that you want to test and click Test LBDN in the Toolbar.
3. In the Test DTC LBDN dialog box, complete the following:
   - Query Source: Enter the client IP address.
   - Query Name: Enter the FQDN of the record that you are requesting.
   - Member: Click Select to select the Grid member that will return the response. The dialog box displays the list of members that have a DTC license.
   - Record Type: Select a record type, A, AAAA, or NAPTR from the drop-down list.
4. Click Start.

The appliance displays the response for the request in the text output area. To clear the response from the text area, click Clear.
Deleting DNS Traffic Control Objects

You can delete DNS Traffic Control objects, such as servers, pools or LBDNs. When you delete an LBDN, the appliance automatically dissociates it from the zones. To delete an LBDN, you must either have a write permission on the LBDN record or the LBDN. For more information, see License Requirements and Admin Permissions.

You cannot delete a DNS Traffic Control pool when it is in use. To delete a pool, you must first delete it from the associated LBDNs. You cannot delete a DNS Traffic Control server when it is in use. You must first remove it from every pool and topology ruleset before deleting the server.

To delete an object:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab, click the Action icon next to the object name and select Delete from the menu or select an object and click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes to delete or No to cancel.

The Delete Confirmation dialog box displays information about associated objects and warns if the object cannot be deleted due to the associations.

To schedule an object deletion, click the Action icon for the object and select Delete -> Schedule Delete. Alternatively, you can select the object in the Traffic Control panel and then select the Delete icon -> Schedule Delete. In the Schedule Deletion panel, enter a date, time, and time zone. For information, see Scheduling Deletions.

Viewing DNS Traffic Control Objects

Grid Manager lists all DNS Traffic Control objects in the Traffic Control tab. You can view the DNS Traffic Control objects, such as servers, LBDNs, and pools that you have configured in the Grid.

To view DNS Traffic Control objects, from the Data Management tab, select the DNS tab -> Traffic Control tab.

Based on the selected columns, Grid Manager displays the following information for each DNS Traffic Control object:

- **Name**: The name of the object.
- **Type**: The object type.
- **Status**: Displays information about the last update, connection status, load balancer methods, and servers and pools. Hover your mouse over the status value to view full information in a tooltip. For more information about the possible statuses, see Understanding DTC Object Status.
- **IPv4Address**: The IPv4 address of the object, if applicable.
- **IPv6Address**: The IPv6 address of the object, if applicable.
- **Disabled**: Yes or No. Indicates whether the DNS Traffic Control object is disabled.
- **Comment**: Displays any comments that were entered for the object.
- **LastStatusUpdate**: Displays the timestamp of the last status update.
- **LoadBalancingMethod**: Displays the load balancing methods defined for the object.
- **TopologyRuleset**: Displays the topology ruleset defined for the object, if the object uses the Topology load balancing method.
- **Extensible attributes, if configured:**
  - **Site**: Displays any values that were entered for the Site pre-defined attribute.
  - **IBDiscoveryOwned**: Displays any values that were entered for the IB Discovery Owned pre-defined extensible attribute.
  - **Building**: Displays any values that were entered for the Building pre-defined attribute.
  - **Country**: Displays any values that were entered for the Country pre-defined attribute.
  - **Region**: Displays any values that were entered for the Region pre-defined attribute.
  - **State**: Displays any values that were entered for the State pre-defined attribute.
  - **VLAN**: Displays any values that were entered for the VLAN pre-defined attribute.

**Note**: You can perform inline editing in the Name, Comment, and Site columns by double-clicking the required line in the table and providing the value in the corresponding column.

You can do the following in the Traffic Control tab:

- Select the check box to view specific objects only:
  - **LBDN**: Select the check box to view LBDN objects only. For more information, see 4820176 4820176.
  - **Pool**: Select the check box to view pools only. For more information, see 4820176 4820176.
  - **Server**: Select the check box to view servers only. For more information, see 4820176 4820176.
- Change the set of columns displayed in the DTC objects table and change their width. For more information, see Customizing Tables.
- Click the Add icon to add an object.
- Select an object and click the Edit icon to edit the configuration. You can also click the Action icon next to the object and select Edit from the menu. For more information, see 4820176 4820176.
- Select an object and click the Delete icon to delete it. You can also click the Action icon next to the object and select Delete from the menu. For more information, see 4820176.
Enabling or Disabling Traffic Control Objects

You can enable or disable multiple traffic control objects simultaneously. To enable or disable traffic control objects:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab.
2. In the Traffic Control panel, select the objects that you want to enable or disable, click the arrow beside the Enable/Disable icon and do one of the following:
   - To enable the selected objects, select Enable from the drop-down list and click Yes in the confirmation dialog box to enable.
   - To disable the selected objects, select Disable from the drop-down list and click Yes in the confirmation dialog box.

Deleting DNS Traffic Control Objects

You can delete DNS Traffic Control objects, such as servers, pools or LBDNs. When you delete an LBDN, the appliance automatically dissociates it from the zones. To delete an LBDN, you must either have a write permission on the LBDN record or the LBDN. For more information, see License Requirements and Admin Permissions.

You cannot delete a DNS Traffic Control pool when it is in use. To delete a pool, you must first delete it from the associated LBDNs. You cannot delete a DNS Traffic Control server when it is in use. You must first remove it from every pool and topology ruleset before deleting the server.

To delete an object:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab, click the Action icon next to the object name and select Delete from the menu or select an object and click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes to delete or No to cancel.

To schedule an object deletion, click the Action icon for the object and select Delete -> Schedule Delete. Alternatively, you can select the object in the Traffic Control panel and then select the Delete icon -> Schedule Delete. In the Schedule Deletion panel, enter a date, time, and time zone. For information, see Scheduling Deletions.

Visualization for DNS Traffic Control Objects

Grid Manager provides a visual tree view that you can use to quickly understand an overall traffic control structure of a selected DTC object. The visualization panel is displayed by default on the Traffic Control tab.

To view a visualization of the DNS traffic control structure for an object:

1. From the Data Management tab, select the DNS tab -> Traffic Control tab.
2. Select the check box for an object which DTC structure you want to view, for example, an LBDN, pool, or server. The LBDN, pool, or server DTC structure tree is displayed in the visualization panel.

The tree shows the selected object and its relationships with other associated DTC objects. The DTC objects are represented as nodes in the hierarchical order of LBDN -> pool -> server levels. Note that when a DTC server is associated with multiple pools, the appliance displays the connection to the selected pool only, not showing the other pools that the server is assigned to. If an LBDN has more than one pool associated, it displays the servers for only one pool at a time. Clicking on another pool of the LBDN displays the servers for that pool.

You can hover your mouse over an object to display a tooltip that contains the following information:

- The name and status of the DTC object. For more information about the possible statuses, see Understanding DTC Object Status.
- Load Balancing Method: This is displayed only for LBDN objects.
- Preferred Load Balancing Method: This is displayed only for pool objects.
- Alternate Load Balancing Method: This is displayed only for pool objects.
- Host: The domain name or IP address of a server object.
- Last Updated: The timestamp when the object was last discovered.
- Health Monitors: This displays health monitors status for pools and servers.

The health status displayed for a DTC server includes health monitors assigned through the pool as well as individual health monitors per IP address or domain name of the server, if assigned. For example, monitor_name(monitor_type) for a pool monitor, and...
IP_address_or_FQDN(monitor_type) for an individual server monitor.

- Ratio: Dynamic: In DTC pools and servers visualization, this displays traffic distribution across members and servers with the Ratio: Dynamic load balancing method applied.
- Number of Pools: Shows the number of pools for the LBDN.
- Number of Servers: Shows the number of servers for the pool.
- Used by these LBDNs: Shows all LBDNs that use the pool.
- Used by these Pools: Shows all pools that use the server.

From a DTC object tooltip, you can perform certain actions on the object. For more information, see the next section, 4820192.

To hide or show the visualization panel, click **Hide Visualization** or **Show Visualization** in the Toolbar.

You can also add the default visualization in the visualization panel, and then define the DTC objects. For more information, see 4820192.

**Note:** Grid Manager can display a maximum of 100 nodes for each level associated with the currently visualized node.

### Understanding DTC Object Status

The DTC object status can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status and Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green Icon" /></td>
<td>Running: The object is fully available and operational.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow Icon" /></td>
<td>Warning: The object has a warning message. You can check the syslog for any messages.</td>
</tr>
<tr>
<td><img src="image" alt="Red Icon" /></td>
<td>Error: The object has an error. You can check the syslog for any messages.</td>
</tr>
<tr>
<td><img src="image" alt="Orange Icon" /></td>
<td>Disabled: The object is disabled due to a configuration setting. This may include a few different reasons, such as the &quot;Disable&quot; flag being set, the DNS service not running on the selected member, a zone not assigned to an LBDN, or the LBDN not associated with a zone for the selected DTC member.</td>
</tr>
<tr>
<td><img src="image" alt="Grey Icon" /></td>
<td>Unknown: The DTC object status has not yet been determined.</td>
</tr>
<tr>
<td><img src="image" alt="Black Icon" /></td>
<td>Unlicensed: The object does not have a DNS Traffic Control license.</td>
</tr>
</tbody>
</table>

It may take a few minutes for the status of an object to be updated after a configuration change.

Grid Manager calculates the status differently for the DTC objects list view and the visualization. For information, see the next section, 4820192.

### Calculating the Status

A DTC pool may use multiple health monitors and it has an availability option for these monitors that is used to determine the status of a DTC server. For example, if the availability requirement is "All", then the server is considered to be 'Running' if all the pool health monitors report the server as 'Running'. Servers may appear in multiple pools that have different health monitors and different availability settings. Thus, a DTC server status can be different for different pools.

You can filter the DTC objects visualization by all members or a specific member. A DTC Grid member uses health monitors to determine the status of a DTC server. A Grid member is associated with an LBDN if that Grid member is assigned a name server for a zone that is associated with an LBDN. A DTC server is associated with an LBDN if it is part of a DTC pool which is used by the LBDN. Thus, if a DTC Grid member is associated to a DTC server through an LBDN, the Grid member checks the status of the DTC server using the health monitors associated with the DTC server's pool. When the visualization is filtered by a specific DTC Grid member, the displayed status of the DTC servers is the status that was determined by that specific DTC Grid member. When you select **All Members** in the visualization, the displayed status is an aggregated status across all DTC Grid members.

For the DTC objects list view, the status is calculated as follows:

- **Server:** Aggregated status from all pool monitoring across all DTC Grid members.
- **Pool:** Aggregated status for all its servers across all DTC Grid members.
- **LBDN:** Aggregated status for all its pools across all DTC Grid members.

For the visualization panel, the status is calculated as follows:

- **Server:** Status from selected pool monitoring for selected DTC Grid member.
• Pool: Aggregated status for all its servers for selected DTC Grid member.
• LBDN: Aggregated status for all its pools for selected DTC Grid member.

**Note:** If a pool has no health monitors configured, then the servers and pool report a status of 'Running'.

**Working with the Visualization Panel**

You can do the following in the visualization panel:

- Resize the visualization panel in relation to the DTC objects list view by dragging the vertical separator between the panel and the list view.
- Filter the visualization by Grid members associated to DTC objects through LBDNs: In the **Member** drop-down list, select **All Members** or a specific member. For more information about how the object status is determined for all members and for a specific member, see 482 0192. Note that the appliance displays only members that have the DNS Traffic Control license.
- Filter by the DTC status: **All DTC Status** or **Non-Running** only. You can combine this filter with the members filter.
- Zoom the map in and out by moving the Zoom slider. You can also zoom in and out by using the mouse wheel.
- Click the **Adjust tree size to window size** icon to adjust the tree size after you zoomed it in our out.
- Change the tree orientation by clicking the Change Tree Orientation icon. The default orientation is vertical.
- Click the **Expand Visualization** icon to open the DTC structure in a separate window. Alternatively, you can click the Action icon next to the required DTC object in the table and select **Expand Visualization**.
- Click the **Refresh** icon to refresh the tree. You can also select the Auto Refresh check box to turn on auto-refresh.
- Click anywhere in the tree and hold your mouse to drag the tree to a desired location in the panel or window.
- Hover your mouse over an LDBN to display the tooltip and do the following:
  - Test the LBDN.
  - Add an existing pool to the LBDN.
  - Add a new pool to the LBDN.
  - Disable or enable the LBDN.
  - Edit the LBDN.
  - Delete the LBDN.
  - Schedule the deletion of the LBDN.
  - Switch to the LBDN visualization mode if you are currently in the pool visualization mode.
- Hover your mouse over a pool to display the tooltip and do the following:
  - Add the pool to an LBDN.
  - Add an existing server to the pool.
  - Add a new server to the pool.
  - Disable or enable the pool.
  - Edit the pool.
  - Delete the pool.
  - Switch to the pool visualization mode if you are currently in the LBDN or server visualization mode.
- Hover your mouse over a server to display the tooltip and do the following:
  - Add the server to a pool.
  - Disable or enable the server.
  - Edit the server.
  - Delete the server.
  - Switch to the server visualization mode if you are currently in the LBDN visualization mode.

**Adding Default Visualization**

The default visualization allows you to design a DNS Traffic Control structure in the inverse order—first, add a visualization of the default DTC objects structure and create the default disabled objects, and then define the objects one by one.

To add the default visualization:

1. On the **Traffic Control** tab, click the arrow next to the **Add** icon and select **Default Visualization**.

   The default basic DTC objects structure is displayed in the visualization panel. It consists of the default server, pool, and LBDN. By default, they are disabled.

   The corresponding server, pool, and LBDN objects are added in the DTC objects list view.

2. Configure the DTC objects in any of the following ways:
   - Hover your mouse over an object to display the tooltip, click the required button, and make the necessary configurations.
   - In the DTC objects list view, select the required object, click the Edit icon, and make the necessary configurations.

   For information about the configurable properties of DTC objects, see **Managing DNS Traffic Control Objects**.

3. If necessary, configure the topology rulesets, topology database, and DTC health monitors used in your DTC structure. For information, see **Defining Topology Rulesets**, **Importing a Topology Database**, and **Using DNS Traffic Control Health Monitors** correspondingly.

4. After you configured the DTC objects, enable each one of them:
Hover your mouse over an object.
Click Enable in the tooltip.

Once all objects are enabled and all necessary service restarts are performed, the whole DTC structure starts working.

Chapter 24 Configuring IP Routing Options

You can configure multiple IP addresses and enable anycast addressing on the loopback interface of the NIOS appliance, allowing the appliance to function in different network deployments. Configuring non-anycast IP addresses on the loopback interface assists in server migration and network address change. Configuring anycast addresses on the appliance allows you to add redundancy and improve reliability for DNS services. You can use OSPF (Open Shortest Path First), BGP (Border Gateway Protocol), or both, as the routing protocol for anycast advertising.

This chapter contains the following sections:

- Using the Loopback Interface
- Configuring IP Addresses on the Loopback Interface
- Advertising Loopback Addresses to the Network
- About Anycast Addressing for DNS
- Configuring Anycast Addresses
- Best Practices for Configuring Anycast Addresses
- IP Routing Options
  - About OSPF
  - Anycast and OSPF
  - Configuring OSPF on the NIOS Appliance
  - Anycast and BGP4
  - Configuring BGP in the NIOS Appliance
- About BFD (Bidirectional Forwarding Detection)
  - Enabling BFD for OSPF
  - Enabling BFD for BGP Neighbor
  - Creating a BFD Template
  - Enabling and Disabling DNS Health Check Monitor
  - Monitoring with SNMP

Using the Loopback Interface

The loopback interface is a virtual network interface on the appliance. You can do the following on the loopback interface:

- Configure IP addresses to consolidate DNS servers for migration purposes. For information, see Configuring IP Addresses on the Loopback Interface.
- Add anycast addresses to improve the reliability and performance of DNS services in multiple locations. For information, see About Anycast Addressing for DNS.
- Separate DNS traffic by assigning an IP address as the source port for DNS queries. For information, see Specifying Source Ports.

When you use the loopback interface for anycast addressing, the upstream and neighboring routers can continue to advertise anycast addresses without being affected by hardware malfunctions.

To configure non-anycast addresses on the loopback interface, complete the following:

1. Add IP addresses to the loopback interface. For information, see Configuring IP Addresses on the Loopback Interface.
2. Enable DNS services on the loopback addresses. For information, see Specifying Port Settings for DNS and its subtopic, Specifying Source Ports.

To configure DNS anycast addresses and their advertising protocols, complete the following:

1. Add anycast addresses to the loopback interface. For information, see Configuring Anycast Addresses.
2. Configure anycast addressing protocols. For information, see Configuring OSPF on the NIOS Appliance and Configuring BGP in the NIOS Appliance. This is the primary application for routing protocols in the NIOS appliance.
3. Enable the DNS anycast addresses. For information, see Specifying Port Settings for DNS and its subtopic, Specifying Source Ports.

To separate DNS queries from DNS transfers and notify messages, complete the following:

1. Add an IP address of the source port for DNS queries. For information, see Configuring IP Addresses on the Loopback Interface.
2. Select the source IP for DNS queries. For information, see Specifying Source Ports.

Configuring IP Addresses on the Loopback Interface

You can configure IP addresses on the loopback interface to minimize service downtime during a server migration. As illustrated in 4820202, you have two existing DNS servers (ns1.corpxyz.com 192.204.18.11 and ns2.corpxyz.com 192.204.18.12) and you want to replace these servers with a new one (ns3.corpxyz.com 192.204.18.88). The migration takes a few weeks and you want DNS services to be available on all three addresses during the migration. You can add all three IP addresses to the loopback interface of a NIOS appliance, and then configure the appliance to provide DNS services on all addresses. After the server migration, you can shut down the old servers and use the new one for services.
You can also add an IP address that is used solely for DNS queries, to separate the DNS traffic. You first add an IP address you want to use for DNS queries on the loopback interface. You then configure the appliance to listen for DNS queries solely on this address. For information, see Specifying Source Ports.

When you configure non-anycast addresses on the loopback interface, ensure that you establish a static route between the appliance and the router so queries to these addresses are routed correctly. For information, see 4820202.

Note: You can configure multiple interfaces on the Infoblox-4030 appliance only. To configure LAN1, LAN2 and MGMT interfaces to the same IPv4 or IPv6 subnet, provide the same netmask for IPv4, or a CIDR prefix for IPv6, as the LAN1 interface. Alternatively, you can use a /32 netmask (255.255.255.255) for IPv4, or /128 CIDR prefix for IPv6 with the same subnet as LAN1 interface to configure multiple interfaces. An Infoblox-4030 can replace three DNS cache servers that are active on the same network. When you configure multiple interfaces on the same subnet, the outgoing traffic from NIOS host which is received through LAN2 and MGMT is directed to the LAN1 router for all interfaces on the LAN1 subnet, irrespective of the destination IP. However, if the LAN1 interface fails, the outgoing traffic will not be re-directed to any other interface and access to LAN2 and MGMT also fails.

To configure an IP address on the loopback interface:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box -> Edit icon.
2. In the Grid Member Properties Editor, select the Network tab -> Basic tab. You can add an IPv4 or IPv6 address on the loopback. You define each type in their own table.
3. Click the Add icon in the Additional Ports and Addresses table and select Additional Address (loopback) (IPv4) or Additional Address (loopback) (IPv6) from the drop-down list.

Note: You cannot configure Additional Address (loopback) (IPv4) interface for an IPv6 Grid member and Additional Address (loopback) (IPv6) interface for an IPv4 Grid member. You can only enter the IP address you want to add to the loopback interface. You cannot configure the subnet mask, prefix length, gateway, or port settings.

The appliance adds a row to the table. Complete the following:

- **Interface:** Displays Additional Address (loopback). You cannot modify this.
- **Address:** Enter the IP address you want to add to the loopback interface. An IPv6 address is a 128-bit number in colon hexadecimal notation. It consists of eight 16-bit groups of hexadecimal digits separated by colons (example: 2001:db8::0000:0123:4567:89ab:0000:0cdef or 2001:db8::123:4567:89ab:0::cdef). For Infoblox-4030 appliance, use a /128 CIDR for IPv6 while configuring multiple interfaces.
- **Subnet Mask (IPv4) or Prefix Length (IPv6):** You cannot change the netmask of the loopback interface. It is set to 255.255.255.255, or /32. For an IPv6 address, the mask is set to 128 and cannot be modified.

Note: You cannot configure the gateway address and port settings.
4. Save the configuration and click **Restart** if it appears at the top of the screen.

To add multiple IP addresses on the loopback interface, repeat the steps for each IP address.

**Note:** If you are configuring the loopback interface on a Grid Master, the Grid is temporarily disrupted upon saving the configuration and restarting services on the appliance. The Grid reconnects automatically and the appliance regains the role as Grid Master after a short delay.

---

**Advertising Loopback Addresses to the Network**

Advertising IP addresses on the loopback interface relies on the upstream router to populate routes to the loopback interface. As illustrated in **482 0202**, when a client on a different subnet queries an IP address on the loopback interface, it sends the request to the router. If the IP address on the loopback interface is not advertised to the router, the request cannot reach the appliance. Therefore, when you configure non-anycast addresses on the loopback interface, or if OSPF or BGP is not configured within your network, you must configure the upstream router to reach the NIOS appliance through a static route on the LAN1 interface.

Note that when an appliance is configured for both authoritative and recursive queries, you should connect your internet interface through the LAN1 port to allow for maximum flexibility while using auxiliary LAN2 and MGMT ports. Consult with your network administrator for information about configuring static routes from the router to the additional IP addresses on the loopback interface.

---

**About Anycast Addressing for DNS**

Note: This feature is not supported on vNIOS appliances for Riverbed.

---

Four types of communications are utilized within an IP network:

- **Unicast** describes a one-to-one network communication between a single sender and a single recipient. The routing protocol determines the path through the network from the sender to the recipient based on the specific protocol or routing scheme. Unicast also describes the address type assigned to the recipient.

- **Multicast** describes a one-to-many network communication between a single sender and a specific group of recipients. All members within the group are intended recipients and each member receives a copy of the data from the sender. Multicast also describes the address type assigned to a group of recipients, used by the routing protocol to determine the path to the group.

- **Broadcast** is similar to multicast, the exception being that data is sent to every possible destination regardless of the groups or subnetwork. There is no specific group of recipients.

- **Anycast** describes a one-to-nearest communication between a single sender and the nearest recipient within a group. The routing protocol chooses one recipient within a target group based on the routing algorithm for the specific protocol, and sends data to that recipient only.

The NIOS appliance provides the following support for DNS anycast addressing:

- You can configure up to 20 anycast IP addresses on the loopback interface of each Grid member.
- Anycast IP addresses can be in IPv4 or IPv6 format. For all anycast IP addresses, the subnet mask value is always set to /32 for an IPv4 anycast IP or 128 for a 128-bit IPv6 address. These values are separate and distinct from the IP configuration on the NIOS appliance LAN port.
- The appliance advertises routing information of the anycast addresses through OSPF or BGP, or (seldom) both, depending on the deployment. Routers use the configured routing protocols to determine the best path to the nearest server. The appliance advertises the route information to the upstream or neighboring router, a router that forwards data on the network link and determines the forwarding path to destinations. For information, see **IP Routing Options**.
- The appliance advertises and withdraws route information based on reachability information to DNS servers sent by the IP route advertisements.
- When you configure DNS anycast addressing on an appliance and use it as an NTP server, the appliance can answer NTP requests through the anycast IP address. For information about how to configure an appliance as an NTP server, see **Configuring a NIOS Appliance as an NTP Server**.

Anycast addressing for DNS provides the following benefits:
• **Improved Reliability**: Anycast provides improved reliability because DNS queries are sent to an anycast IP address that is defined on multiple DNS servers in the NIOS Grid. If the nearest server somehow goes offline, then the router forwards the request to the next nearest DNS server advertising the target anycast IP address (see Figure 24.4 for an example).

• **Load Distribution**: Anycast distributes the load across multiple DNS servers based on network topology.

• **Improved Performance**: The NIOS appliance uses OSPF or BGP, depending on your configuration, to advertise anycast routing information to the upstream and neighboring routers. The routers determine the best route to the nearest DNS server. Anycast enables the queries to reach the nearest server more quickly, providing faster responses to DNS queries.

**Note**: For more information about anycast addressing, refer to RFC 1546 "Host Anycasting Service".

### Configuring Anycast Addresses

Anycast addressing is supported on loopback interfaces on the NIOS appliance. IP configuration must be defined on the LAN1 interface before configuring anycast IP addresses. Before creating IPv6 anycast IPs on the loopback interface, IPv6 must be enabled and configured on the LAN1 interface for the NIOS appliance, including the correct IPv6 gateway IP address.

**Note**: When you add an anycast address, you need to start the service for the advertising to take place. However, when you remove an anycast address, no service restart is required to stop the service. Anycast advertising stops immediately.

To enable and configure anycast addressing:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid member check box -> Edit icon.
2. In the Grid Member Properties editor, Click Toggle Advanced Mode.
3. When the additional tabs appear, click the Anycast tab.
4. Click the Add icon and choose IPv4 Address or IPv6 Address.
5. In the Anycast Interfaces list, enter the values or select the options for the new entry:
   - **Anycast Interface**: Anycast addressing is supported on the loopback only. This value is filled in automatically.
   - **Address**: Enter the IP address you want to assign as the anycast IP address to the loopback interface. Specify an IPv4 Address or an IPv6 Address based on the chosen type of address.
   - **Subnet Mask**: You cannot change the subnet mask of a loopback interface. The netmask is automatically set to 255.255.255.255, or /32; or 128 for IPv6.
   - **OSPF**: Select if you want the appliance to use OSPF to advertise the anycast address, and if necessary configure the OSPF settings. For information, see Configuring OSPF on the NIOS Appliance. IPv4 and IPv6 options are configurable for this protocol. This is supported only for IPv4 and dual mode appliances, but not for IPv6 appliances.
   - **BGP**: Select this if you want the appliance to use BGP to advertise the anycast address, and then configure the BGP settings. This is supported only for IPv4 and dual mode appliances, but not for IPv6 appliances.

**Note**: You must configure at least one routing method for DNS anycast. You can configure OSPF, BGP, or both (in most cases only one protocol will be used). The appliance cannot save the anycast address if you do not complete at least one routing configuration. Anycast cannot be used without dynamic routing.

- **Comments**: Enter a text string to help identify this interface and IP address.

6. **If using OSPF for the current appliance**: Under OSPF Area Configuration, click the Add icon. A new configuration block appears in the properties editor.
   - Enter the values for the OSPF configuration as described in the section Configuring OSPF on the NIOS Appliance.
   - Click the Add down arrow icon in the OSPF Area Configuration section. The new OSPF configuration is saved into a table.

7. **If using BGP for the current appliance**: In the properties editor, scroll down to the configuration block for BGP Configuration. For information, see Configuring BGP in the NIOS Appliance.
   - In the ASN field, enter the Autonomous System ID number in which the NIOS appliance resides.
   - If necessary, modify the BGP Timer Keep Alive and Hold Down values. In most circumstances these values should be left at their defaults. Check your network's defined policies for the desired values if necessary.
   - Click the Add icon.
   - Enter the Neighbor Router IP address. This can be an IPv4 address or an IPv6 address.
   - Enter the Remote ASN (Autonomous System ID number) for the adjacent router.

8. Save the configuration. The system will warn that you must restart the appliance services in order to use the new configuration.

9. Log back in to the appliance.

10. From the Data Management tab, select the DNS tab -> Members/Servers tab -> Grid member check box -> Edit icon.

11. Select Toggle Advanced Mode (if necessary), click General and the Advanced tab.

12. **Under Listen on these additional IP addresses**, click the Add button. The list of one or more previously created IPv4 and IPv6 addresses for the loopback interfaces (created in Step 4) appear in this table. (If the Add button is not active here, this indicates that you have not configured any loopback interfaces with their IP addresses.) Should you need to configure other DNS properties on this page, see...
13. Click **Save and Close**.

Configured anycast interfaces are now enabled to carry DNS traffic. For further information, see **Specifying Source Ports**.

**Best Practices for Configuring Anycast Addresses**

Infoblox highly recommends that you do the following before you configure an Anycast address:

- Enable the Anycast feature in the NIOS application.
- Install a valid DNS license, enable DNS and ensure that the DNS service is active.
- When you configure OSPF or OSPFv6, ensure that the OSPF monitor runs every four seconds.
- You must configure an IP address on the loopback interface.

**IP Routing Options**

IP routing is a set of protocols that determine the path IP packets follow in order to travel across multiple networks from the source to the destination. When information travels through a series of routers and across multiple networks, IP routing protocols enable the routers to build up a forwarding table that correlates the final destination with the next upstream routers.

For routing purposes, the internet is divided into ASs (Autonomous Systems). Data is routed within an AS using an IGP (Interior Gateway Protocol) and routed between different ASs using an EGP (Exterior Gateway Protocol). NIOS appliances support OSPFv2 (for IPv4) and OSPFv3 (for IPv6) for a routing IGP, and BGP4 to advertise DNS anycast addresses in the larger internetwork.

As noted in the section **Configuring Anycast Addresses**, you configure OSPF or BGP4 to advertise anycast addresses, which configured on the loopback interface of NIOS appliances. Use of either protocol depends on the network topology, based on whether the advertisements will propagate only within a single AS or between more than one AS. 

*Figure 24.3 OSPF and BGP Routing Example*

Within each AS, OSPF is the protocol used to forward anycast advertisements. Between ASs, BGP is the protocol selected to advertise anycast addresses. Using this technique, DNS servers in diverse locations can operate together to ensure continuous service.

About OSPF
OSPF is a link-state protocol based on the Dijkstra algorithm used to calculate the shortest path to a destination address within an internetwork. This protocol uses a link-state database created using routing information advertised from neighbors and peers, each with costs based on the state of that link to the destination.

OSPF network topologies consist of administrative domains called OSPF areas. An area is a logical collection of OSPF routers, servers and other network devices that have the same area identifier. A router within an area keeps an OSPF database for its OSPF area only, reducing the size of the database that is maintained.

**Anycast and OSPF**

NIOS appliances can use the OSPF routing protocol to advertise routes for DNS anycast addresses to an upstream router within the autonomous system. The upstream router uses the OSPF advertisement to determine the nearest DNS server from a group of servers within the internetwork. In practice, the NIOS appliance relies upon OSPF to determine the best route for DNS queries to take to the nearest DNS server. The upstream router then forwards the query to the chosen DNS server.

As illustrated in 4820210, to enable anycast for DNS queries, you configure two or more DNS servers within the AS routing domain with the same anycast address on their loopback interfaces. When you select OSPF as the routing protocol, the upstream router determines the nearest server within the group of servers configured with that anycast address. (The "nearest" DNS server may not necessarily be the geographically closest DNS server; it is the DNS server with the lowest cost associated with its reachability from the current node. This is calculated through the OSPF routing algorithm, a discussion of which is far beyond the scope of this manual.) The nearest DNS server configured with the correct anycast address then responds to the DNS query. In the case where the nearest server becomes unavailable, the next nearest server responds to the query. OSPF anycast provides a dynamically routed failover to ensure that DNS can always resolve client requests within the AS. From the client perspective, anycasting is transparent and the group of DNS servers with the anycast address appears to be a single DNS server.

Figure 24.4 Anycast Addressing for DNS Using OSPF

After you configure or change DNS anycast settings, you must restart the DNS services for the settings to take effect. When you enter any OSPF command and wait for the interface to return more information, the appliance disconnects your CLI session after you restart services or make other OSPF configuration changes through Grid Manager. Re-enter your credentials to log back in to the CLI. (For information, refer to the Infoblox CLI Guide.)

To enable the appliance to support OSPF and advertising anycast addresses on OSPF from the loopback, you must first configure the LAN1 or LAN1 (VLAN) interface as an OSPF advertising interface. For information about VLAN, see About Virtual LANs.

You can also configure authentication for OSPF advertisements to ensure that the routing information received from a neighbor is authentic and the reachability information is accurate. This process can be implemented for OSPF over IPv4 networks but is not supported for IPv6/OSPFv3.

For information, see 4820210.

**Note:** For more information about the OSPF routing protocol, refer to RFC 2328 "OSPFv2" and RFC 5340 "OSPF for IPv6".
Configuring OSPF on the NIOS Appliance

**Note:** Use the CLI command `show ospf` or `show ipv6_ospf` to display configuration and statistical information about the OSPF protocol running on the appliance. You can also use the `set ospf` or `set ipv6_ospf` command to write OSPF statistical information to the syslog. In the NIOS appliance, configuration of OSPF is limited to Syslog and the DNS anycast application.

To support DNS anycast and other routing-dependent applications on NIOS appliances, you must first configure the LAN1 or LAN1 (VLAN) interface as an OSPF advertising interface, and then assign an area ID on the interface to associate it with a specific OSPF area. The interface advertises the OSPF routing information to the network so that routers can determine the best server to query. Note that the appliance automatically uses the HA interface as the advertising interface for an HA pair, even though you select the LAN1 interface. For anycasting, the advertising interface sends out routing advertisements about the anycast address into the network out to upstream routers.

**Note:** IPv6 is not supported for the Stub and Not-so-stubby area types.

To configure the LAN1 (HA) or LAN1 (VLAN) interface to be an OSPF advertising interface, perform the following tasks:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.
2. Select the Anycast tab in the Grid Member Properties editor.
   The Anycast Interfaces appear in a table. You can add new anycast interfaces when needed.
3. Click the Add icon of the OSPF Area Configuration table and choose IPv4 Configuration or IPv6 Configuration to define a new OSPF Area. The OSPF Area Configuration will show a similar set of Add (IPv4/IPv6) OSPF Area configuration settings based on the protocol type. Enter the following information to configure the LAN1, or LAN1 (VLAN) as the OSPF advertising interface:
   - **Advertising Interface:** Displays the interface that sends out OSPF routing advertisement. OSPF advertisements are supported on the LAN1 and LAN1 (VLAN) interfaces. For an HA pair, select LAN1 and the appliance automatically uses the HA interface as the advertising interface.
   - **Area ID:** Enter the OSPF area identifier of the network containing the upstream routers, in either an IP address format or a decimal format. All network devices configured with the same OSPF area ID belong to the same OSPF area. The area ID configured on the Grid member must match the area ID of the upstream router configuration. Area ID numbers are defined in the same format for IPv6 and IPv4.
   - **Area Type:** Select the type of OSPF area to associate with the advertising interface from the drop-down list. The area type configured on the Grid member must match the area type of the upstream router configuration. The supported area types are described as follows:
     - **Standard:** A standard area has no restrictions on routing advertisements, and connects to the backbone area (Area 0) and accepts both internal and external link-state advertisements.
     - **Stub:** A stub area is an area that does not receive external routes.
     - **Not-so-stubby:** A not-so-stubby area (NSSA) imports autonomous system (AS) external routes and sends them to the backbone, but cannot receive AS external routes from the backbone or other areas.

**Note:** OSPF for IPv6 (known as OSPFv3) configuration does not support OSPF authentication options.

- **Authentication Type:** Select the authentication method to use to verify OSPF routing advertisements on the interface. The authentication type configured on the Grid member must match the authentication type of the upstream router configuration. The supported authentication types are described as follows:
  - **None:** No authentication for OSPF advertisement.
  - **Simple:** A simple password for OSPF advertisement authentication, in clear text.
  - **MD5:** An MD5 hash algorithm to authenticate OSPF advertisements. This is the most secure option.
  - **Authentication Key ID:** Enter the key identifier to use to specify the correct hash algorithm after you select MD as your OSPF authentication type. The authentication key ID configured on the Grid member must match the authentication key ID of the upstream router configuration.
  - **Authentication Key:** Enter the authentication password to use to verify OSPF advertisements after you select Simple or MD as your OSPF authentication type. Specify a key string between 1 to 8 characters for Simple authentication, and a string between 1 to 16 characters for MD5 authentication. The authentication key configured on the Grid member must match the authentication key of the upstream router configuration.
  - **Cost:** Select one of the following:
    - **Calculate Automatically:** Select this check box to auto generate the cost to associate with the advertising OSPF interface to the appliance. If this check box is not selected, then you specify the cost value explicitly. Calculate the cost as 100,000,000 (reference bandwidth) divided by the interface bandwidth. For example, a 100Mb interface has a cost of 1, and a 10Mb interface has a cost of 10.
    - **Fixed Metric:** Enter the cost to associate with the advertising OSPF interface to the appliance.
  - **Hello Interval:** Specify how often to send OSPF hello advertisements out from the appliance interface, in seconds. Specify any number from 1 through 65,535. The default value is 10 seconds. The hello interval configured on the Grid member must match the hello interval of the upstream router configuration.
  - **Dead Interval:** Specify how long to wait before declaring that the NIOS appliance is unavailable and down, in seconds. Specify any number from 1 through 65,535. The default value is 40 seconds. The dead interval configured on the Grid member must match the dead interval of the upstream router configuration.
  - **Retransmit Interval:** Specify how long to wait before retransmitting OSPF advertisements from the interface, in seconds. Specify any number from 1 through 65,535. The default value is 5 seconds. The retransmit interval configured on the Grid member must match the retransmit interval of the upstream router configuration.
  - **Transmit Delay:** Specify how long to wait before sending an advertisement from the interface, in seconds. Specify any number...
from 1 through 65,535. The default value is 1 second. The transmit interval configured on the Grid member must match the transmit interval of the upstream router configuration.

- **Click Add** to add the interface to the table.

**The Cost, Hello Interval, Dead Interval, Retransmit Interval** and **Transmit Delay** settings can be configured for IPv6 deployments. OSPF authentication is not supported for IPv6 on the NIOS platform.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Managing OSPF

- OSPF advertises the route when the DNS service starts. The start DNS command creates an interface and starts the OSPF daemon.
- OSPF stops advertising the route when the DNS service stops. The stop DNS command stops the OSPF daemon and deletes the interface.
- The NIOS application does not support a route flap. For example, temporary DNS downtime such as restart, does not stop or re-instantiate the OSPF advertisement.
- The OSPF advertisement stops if DNS service is down for more than 40 seconds.

### Anycast and BGP4

**Note:** Use the CLI command **show bgp** or **show ipv6_bgp** to display configuration and statistical information about the Border Gateway Protocol running on the appliance. You can also use the **set bgp** command to write OSPF statistical information to the syslog. In the NIOS appliance, configuration of BGP is limited to Syslog and the DNS anycast application.

BGP (henceforth referred to as BGP) is designed to distribute routing information among ASs and exchange routing and reachability information with other BGP systems using a destination-based forwarding paradigm. Unlike OSPF, which calculates routes within a single AS, BGP is a vector routing protocol that distributes routing information among different ASs. A unique ASN (autonomous system number) is allocated to each AS to identify the individual network in BGP routing. A BGP session between two BGP peers is an eBGP (external BGP) session if the BGP peers are in different ASs. A BGP session between two BGP peers is an iBGP (internal BGP) session if the BGP peers are in the same AS.

BGP configuration enables large enterprises using BGP as the internetworking protocol to provide resilient DNS services using the Infoblox solution. While BGP is mostly used by ISPs, it is also used in larger enterprise environments that must interconnect networks that span geographical and administrative boundaries. In these environments, it is required to use BGP to advertise anycast routes. Using BGP allows the appliance to advertise DNS anycast addresses to neighboring routers across multiple ASs that also use BGP as their routing protocols.

As illustrated in 4820210, to enable anycast for DNS queries among three different networks that span different geographical regions, you can configure two DNS servers with the same DNS anycast addresses in the AS 65497 network. Since other network routers in AS 65498 and AS 65499 also use BGP as the routing protocol, the DNS anycast addresses can be advertised across these networks.

**Figure 24.5 Anycast Addressing for DNS using BGP**

To enable DNS anycast addressing across different ASs, you configure BGP as the routing protocol on the NIOS appliance. (As illustrated in 4820210, the AS 65497 network contains the Infoblox DNS anycast servers, and the AS 65499 network contains Router 1 and 2. The routers use BGP and are peered with the DNS servers. You can configure anycast addressing on the loopback interface of the DNS servers and select BGP as the protocol to advertise the anycast addresses to Router 1 and 2 in AS 65499. For information, see Configuring Anycast Addresses. Once you have configured the DNS servers, the appliances automatically add filters on the advertising interfaces to limit the advertisements to the configured anycast IP addresses. Similarly, BGP filters are applied to ensure that the DNS servers only receive default route advertisements from the neighboring routers.

**Figure 24.6 Anycast and BGP Configuration on Infoblox Appliances**
BGP uses timers to determine how often the appliance sends keepalive and update messages, and when to declare a neighboring router out of service. You can configure the time intervals for these timers. For information, see \[4820210\].

The BGP protocol service is automatically configured to send SNMP queries about BGP runtime data. The appliance sends SNMP traps to its neighboring routers when it encounters issues with the protocol. BGP is configured to send SNMP traps as defined in RFC4273 Definitions of Managed Objects for BGP-4. You must enable and configure the SNMP trap receiver on the Grid member for the member to send SNMP traps. For information, see SNMP MIB Hierarchy. You can use the set bgp command to set the verbosity levels of the BGP routing service. The appliance writes BGP statistical information to the syslog. After you configure the settings, you must restart the DNS services for the settings to take effect. For information, refer to the Infoblox CLI Guide. Note that when you enter any BGP command and wait for the interface to return more information, the appliance disconnects your CLI session if you restart services or make other BGP configuration changes through Grid Manager. You must re-enter your credentials to log back in to the CLI.

You can configure BGP on any interface to advertise anycast addresses across multiple ASs.

**Note:** NIOS selects the interface for BGP advertisement based on the routing configuration.

The appliance supports BGP version 4. For more information about BGP, refer to RFC4271, A Border Gateway Protocol 4 (BGP-4).

## Configuring BGP in the NIOS Appliance

You can configure the appliance as a BGP advertising interface for anycast addresses. The NIOS appliance advertises the BGP routing information to the network so routers can determine the nearest server to query. The NIOS appliance does not perform dynamic routing itself; it can use dynamic routing protocols to advertise its DNS anycast availability. You must define the ASN of the interface and list any neighboring routers that will receive the BGP announcements. On an HA pair, BGP runs only on the active node. In an HA failover, the BGP service resumes on the new active node.

**Note:** If you encounter Malformed AS_PATH error, then remove the dont-capability-negotiate option. Infoblox doesn’t provide an option to create confederation of autonomous systems if the BGP peer is configured by enabling the dont-capability-negotiate option.

## Authenticating BGP Neighbors

You can configure authentication for BGP advertisements to avoid any malicious interference by ASs. This ensures that the routing information exchanged between BGP peers is authentic, and it is accepted only if the authentication is successful. BGP authentication must be configured with the same password on both BGP peers. Otherwise, the connection between them is not established. The Infoblox BGP authentication fully conforms to RFC 2385. For information about BGP authentication, refer to RFC 2385, Protection of BGP Sessions via the TCP MD5 Signature Option.

**Note:** If you upgrade from a previous NIOS version to NIOS 6.11.0 or later, BGP authentication is disabled for existing BGP neighbors.
The BGP service restarts automatically when any of the following authentication changes are made:

- MD5 authentication is enabled or disabled for a BGP neighbor.
- Change the authentication password of a BGP neighbor, for which MD5 authentication is enabled.

To configure BGP for anycast addresses:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.
2. In the Grid Member Properties editor, select the Anycast tab.
3. In the BGP Configuration section, complete the following:
   - Interface Link Detection: Select this check box to enable link detection when the default connection fails. This enables the router to track the next available route. For example, if LAN1 is set as the default gateway when both LAN1 and LAN2 are working, and LAN1 later fails, the router will switch to LAN2. When LAN1 reconnects, the router will then switch back to LAN1.
   - ASN: Enter the autonomous system number of the interface. Enter a number from 1 to 65535. You can configure only one ASN on each Grid member.
   - BGP Timers: BGP uses timers to control how often the interface sends KEEPALIVE messages and how long it waits before declaring a neighboring router out of service. The keepalive timer determines the time interval at which the interface sends KEEPALIVE messages to a neighboring router to inform the neighbor that the appliance is alive. The hold down timer determines how long the interface waits to hear a KEEPALIVE or UPDATE message before it assumes the neighbor is out of service. If a neighboring router is down, the interface terminates the BGP session and withdraws all the BGP routing information to the neighbor.
     - Keep Alive: Enter the time interval in seconds when the interface sends keepalive messages. You can enter a time from 1 to 21845 seconds. The default is four seconds.
     - Hold Down: Enter the time in seconds that the interface waits to hear a keepalive message from its neighbor before declaring the neighbor out of service. You can enter a time from 3 to 65535 seconds. The default is 16 seconds.

Click the Add icon to add a neighboring router to receive BGP advertisements from the NIOS appliance. The appliance adds a new row to the table. Complete the following:

- Neighbor Router IP: Enter the IP address (IPv4 or IPv6) of the neighboring BGP router. The neighboring router can be within the same AS (the most likely case) or from a router in an external AS.
- Remote ASN: Enter the ASN of the neighboring router. You can enter an ASN number from 1 to 65535.
- MD5 Authentication: Select this check box to enable MD5 authentication for the BGP neighbor. When you enable MD5 authentication, you must enter the authentication password in the Password field.
- Password: Enter the authentication password that the NIOS appliance uses to connect to the BGP neighbor. You can enter up to 80 printable ASCII characters. The password configured on the Grid member must match the password of the BGP neighbor.

Note: When you enter the password for a BGP neighbor, it will be preserved even if you disable MD5 authentication for the BGP neighbor later. But if you change the IP address for any existing BGP neighbor, you must re-enter the authentication password for the BGP neighbor, even if the authentication password remains the same.

- Comment: Enter useful information about this neighboring router.

Click the Add icon again to add another neighboring router. You can add up to 10 neighboring routers.

4. Save the configuration and click Restart if it appears at the top of the screen.

5. Anycast configuration is complete. To activate anycast, see Specifying Port Settings for DNS and its subtopic, Specifying Source Ports.

About BFD (Bidirectional Forwarding Detection)

NIOS supports Anycast addressing for DNS using BGP and OSPF routing protocols. Since BGP and OSPF have timer granularity in seconds, the network re-convergence is slow in case of faults in forwarding path. BFD protocol is designed to provide faster failure detection using millisecond timer intervals. It can be enabled with routing protocols to achieve fast network re-convergence. BFD can be enabled for OSPF or BGP and you can create BFD templates and assign it to OSPF Area or BGP neighbors. You can enable BFD simultaneously for OSPF and BGP, but only one BFD session will be created for a given neighbor. Infoblox recommends you to use the same BFD template for both OSPF and BGP neighbor whenever such a configuration is required.

The BFD protocol feature is supported in NIOS 8.0.0 and later releases. For more information about loopback interface (anycast), DNS, BGP, and OSPF configuration, refer to the Infoblox NIOS Administrator Guide.

This document provides a brief overview about enabling BFD for OSPF Area and BGP Neighbors, creating BFD templates, SNMP, and CLI commands.

WARNING: The default advertised setting for BFD holddown is 300 ms (100 ms transit/receive intervals and detection multiplier 3). This setting is optimized for typical routers and directly connected endpoint configurations. If your network requires an implementation of L2 multi-path or port redundancy, you must adjust the holddown interval value higher than the spanning-tree rebalance latency to avoid unnecessary changes to the L3 network topology or the forwarding path for DNS traffic.

Enabling BFD for OSPF
You can enable BFD for IPv4 or IPv6 OSPF Area. To support DNS anycast and other routing-dependent applications on NIOS appliances, you must first configure the LAN1, LAN1 (VLAN), or HA (for HA pairs only) interface as an OSPF advertising interface, and then assign an area ID on the interface to associate it with a specific OSPF area. For more information, refer to the NIOS Administration Guide.

To enable BFD for IPv4 or IPv6 OSPF Area:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.
2. In the Grid Member Properties editor, select the Anycast tab.
3. In the OSPF Area Configuration table, select the OSPF advertising interface, click the Edit icon, and then complete the following:
   - Enable BFD: Select this check box to enable BFD for the OSPF advertising interface.
   - BFD template: Click Select BFD Template and select a BFD template from the Select BFD Template dialog box. You can click Clear to remove the selected BFD template and select a new one.
4. Save the configuration.

When OSPF session with a neighbor router in the OSPF Area reaches FULL state, BFD session is automatically created. By default, BFD runs with no authentication and timer intervals of 100ms transmit, 100ms receive and multiplier 3 (hold down time = 300ms). The actual runtime intervals are negotiated with the peer as per BFD standard RFC 5880. If these intervals are not suitable or authentication needs to be enabled for BFD, you must create a BFD Template as described in the section.

Figure 24.7 Enabling BFD for OSPF

You can use the show ipv6 ospf neighbor CLI command to view runtime BFD information for OSPF.

Infoblox > show ipv6 ospf neighbor

Neighbor 10.40.16.16%bond0
    Area 0.0.0.2 via interface bond0 (ifindex 40)
    His IfIndex: 5 Link-local address: fe80::5a8d:9ff:fec2:46b2
    State Full for a duration of 00:12:33
    His choice of DR/BDR 10.40.16.16/10.34.54.68, Priority 1
    Using BFD to detect fast failover
        BFD last signalized state : Up
        DbDesc status: Slave SeqNum: 0x8a63b025
    Summary-List: 0 LSAs
Enabling BFD for BGP Neighbor

BFD can be enabled for each configured BGP neighbor individually. You can also use the Enable Multi-hop option, which allows BGP to connect to BGP neighbors which are more than one IP hops away.

To enable BFD for the BGP neighboring router:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then click the Edit icon.
2. In the Grid Member Properties editor, select the Anycast tab.
3. In the BGP Neighbor Configuration table, select the BGP neighboring router, click the Edit icon, and then complete the following:
   - **Enable Multi-hop (optional)**: Select this check box to allow BGP to connect with the neighbors which are more than one IP hops away.
   - **Hop Limit**: Enter the maximum hop limit. The default value is 255.
   - **Enable BFD**: Select this check box to enable BFD for the BGP neighboring router.
   - **BFD template**: You can assign a BFD template to the BGP neighboring router to run BFD with non-default settings. Click Select BFD Template and select a BFD template from the Select BFD Template dialog box. You can click Clear to remove the selected BFD template and select a new one. For information about creating a BFD template, see 4820225
4. Save the configuration.

BFD session for a given BGP neighbor is created when BGP state reaches ‘Established’.

> Figure 24.8 Enabling BFD for BGP Neighbor

Viewing Runtime BFD Information for BGP

You can use the `show bgp neighbor` CLI command to view runtime BFD information for BGP.

```
Infoblox > show bgp neighbor
BGP neighbor is 10.34.54.16, remote AS 100, local AS 10, external link BGP version 4, remote router ID 10.40.16.16
```
BGP state = Established, up for 00:00:42

Using BFD to detect fast failover in standard mode BFD last signalized state : Added

Last read 00:00:00, hold time is 16, keepalive interval is 4 seconds Neighbor capabilities:

4 Byte AS: advertised and received

Creating a BFD Template

BFD advertises the default hold-down interval of 300ms and authentication is disabled, by default. In order to configure faster or slower hold-down intervals, you can create BFD templates and assign it to the OSPF Area or BGP neighbors. You can configure a BFD template at the Grid level and assign it to multiple Grid members. The BFD template can be assigned to the BGP neighbor or OSPF Area of any Grid member in the Grid and it can be assigned to multiple BGP neighbors or OSPF Areas.

To create BFD templates:

1. From the Grid tab -> Grid Manager tab, expand the Toolbar and click Manage BFD Templates.
2. In the Manage BFD Templates wizard, click the Add icon, and then complete the following:
   - **Name**: Enter the name of the BFD template.
   - **Authentication Type**: Select the authentication type from the drop-down list. You can select one of the following authentication types: MD5, SHA-1, Meticulous MD5, or Meticulous SHA-1. The BFD authentication type fully conforms to RFC 5883.
   - **Authentication Key ID**: Enter the key identifier to use to specify the correct hash algorithm after you select the authentication type. If you do not enter a value here, the appliance by default sets 'one' as the authentication key ID. The authentication key ID configured on the Grid member must match the authentication key ID of the upstream router configuration.
   - **Authentication Secret/Password**: Enter the authentication password to use to verify after you select the authentication type. You can enter password with 4-16 printable ASCII characters. The authentication password configured on the Grid member must match the authentication key of the upstream router configuration.
   - **Intervals**: Specify the following BFD timer intervals for each router interface.
     - **Min Rx Interval (ms)**: Enter the minimum receive interval. The default is 100ms.
     - **Min Tx Interval (ms)**: Enter the minimum transmit interval. The default is 100ms.
     - **Multiplier**: Enter the detection multiplier. You can enter a value between 3 and 50. The default is 3.
3. Click Add.

After you have added BFD templates, you can do the following:

- Select a BFD template and click the Edit icon to edit the configuration.
- Select a BFD template and click the Delete icon to delete it.
Enabling and Disabling DNS Health Check Monitor

In order to minimize downtime for DNS and ensure high availability, NIOS implements DNS process monitoring and self-recovery on each Grid member, in order to minimize downtime for DNS and ensure high availability. You can enable the DNS health check monitor to monitor whether the DNS server is responding to client requests. When you enable this feature, the appliance sends a query to the DNS server and waits for the response until the specified timeout duration. If the appliance is unable to receive a response from the DNS server after the specified number of retries, the appliance sends SNMP traps and email notifications about the failure. The appliance performs the DNS health check periodically based on the specified time interval.

If BFD is used for anycast fault detection, the BFD session state advertised from the member can be in the Down state whenever there is a DNS health check failure. This allows quick anycast route tear-down and the network might converge with another DNS server that can serve same anycast IP.

Additionally, you can also configure domain names in the DNS health check monitor, which are probed simultaneously and if any one of the domains fail to resolve for consecutive attempts, the DNS health is considered as Down. If recursion is enabled on the Grid member, the queries to these domains help to assert the ability of the DNS server to reach the external authoritative servers and optionally trigger network re-convergence in case of a failure. When no domains are configured, local PTR queries are used to probe the DNS process.

WARNING: The DNS Health Check monitor might not work properly if DNS blackhole feature is enabled or if any named ACL is blocking the query sent to the loopback interface.

To enable or disable the DNS health check monitor:

1. Grid: From the Data Management tab, select the DNS tab, and then select Grid DNS Properties from the Toolbar.
   Member: From the Data Management tab, select the DNS tab and click the Members tab -> member check box -> Edit icon.
   In the Grid DNS Properties or the Member DNS Properties editor, click Toggle Advanced Mode if the editor is in the basic mode.
2. Click the Advanced subtab of the General tab and then complete the following:
   - Enable DNS Health Check: This check box is deselected by default, meaning the DNS health check monitor is disabled. Select this check box to enable the DNS health check monitor and specify the following:
     - Interval: Enter the time interval in seconds. The interval value is measured from the end of the previous monitoring cycle. The default is 30 seconds. You can enter a value between 10 and 21600 seconds.
     - Timeout: Enter the timeout value in seconds. This is the time the appliance waits for a response to the query. The default is 3 seconds. You can enter a value between 1 and 10 seconds.
     - Retries: Enter the number of times the appliance tries to send the query after a failed attempt. The default is 3. You can enter a value between 1 and 10.
   - Link BFD session state to DNS Health Check: Select this check box to link the BFD session state with the DNS health check monitor.
   - Resolve Additional Domains: Click the Add icon and enter the domain name. The DNS health check monitor sends recursive queries to the local DNS server (BIND/Unbound) for the domain names listed in this table. You can add up to 16 domain names.
3. Save the configuration.

Note: You must carefully select the domain names for DNS health check monitor with BFD session in order to avoid unnecessary changes in downstream DNS traffic due to transient health check query failures. Setting a higher timeout or retry count might help in avoiding false alarms.
Monitoring with SNMP

Infoblox MIBs (IB-TRAP-MIB, IB-PLATFORMONE-MIB) are updated to include a notification for BFD process failure (ibBFDSoftwareFailure). By default, SNMP notifications are enabled for the BFD process failure event. You can enable or disable SNMP and email notifications for specific event types, by selecting the corresponding check boxes in the Notification tab of the Grid Properties or Member Properties editor.

In addition, BFD process can generate SNMP traps for session state changes according to the standard BFD MIBs described in RFC 7330 and RFC 7331:

- `.1.3.6.1.2.1.222.0.1 (bfdSessUp)`: This notification (aka trap) is sent when one of the neighbors changes the BFD-session state as 'Up.'
- `.1.3.6.1.2.1.222.0.2 (bfdSessDown)`: This notification (aka trap) is sent when one of the neighbors changes the BFD-session state as 'Down' or 'AdminDown.'
.1.3.6.1.2.1.222.1.2.1.13 (bfdSessDiag): The diagnostic code which can be one of the following:
- noDiagnostic (0)
- controlDetectionTimeExpired (1)
- echoFunctionFailed (2)
- neighborSignaledSessionDown (3)
- forwardingPlaneReset (4)
- pathDown (5)
- concatenatedPathReset (6)
- administrativelyDown (7)
- reverseConcatenatedPathDown (8)
- misConnectivityDefect (9)

Note that you must download the following MIBs to enable the trap-receiver to parse the notifications:
- BFD-STD-MIB
- BFD-TC-STD-MIB
- DIFFSERV-MIB
- DIFFSERV-DSCP-TC
- INTEGRATED-SERVICES-MIB
- IANA-BFD-TC-STD-MIB

Part 5 DHCP

This section describes how to configure the Grid to provide DHCP services. It includes the following chapters:

- Chapter 25, Infoblox DHCP Services
- Chapter 26, Configuring DHCP Properties
- Chapter 28, Managing DHCP Templates
- Chapter 27, Managing IPv4 DHCP Data
- Chapter 29, Managing IPv6 DHCP Data
- Chapter 30, DHCP Failover
- Chapter 31, Configuring IPv4 DHCP Filters
- Chapter 32, Authenticated DHCP
- Chapter 33, Managing Leases

Chapter 25 Infoblox DHCP Services

This chapter provides an overview of the Infoblox DHCP services for IPv4 and IPv6. It contains the following sections:

- About Infoblox DHCP Services
- IPv4 DHCP Protocol Overview
- IPv6 DHCP Protocol Overview
  - IPv6 Address Structure
- Configuring DHCP Overview
- Managing DHCP Data
  - About Networks
  - About Shared Networks
  - About DHCP Ranges
  - About Fixed Addresses
  - About Hosts
  - DHCP Configuration Checklists
- About DHCP Inheritance
  - Overriding DHCP Properties
  - Viewing Inherited Values
- About Network Views
  - Adding Network Views
  - Modifying Network Views
  - Deleting Network Views

About Infoblox DHCP Services

DHCP (Dynamic Host Configuration Protocol) is a network application protocol that automates the assignment of IP addresses and network parameters to DHCP-configured network devices (DHCP clients). When a DHCP client connects to a network, it sends a request to obtain an IP address and configuration information from the DHCP server. The DHCP server manages a pool of IP addresses and configuration information such as default gateway, domain name, and DNS server. Depending on the configuration, the DHCP server either assigns or denies an IP address to a client request. It also sends network configuration parameters to the client.

You can configure a NIOS appliance to provide DHCP service for IPv4 and IPv6. The Infoblox DHCP server complies with a number of DHCP and
DHCPv6 RFCs (see Appendix A Product Compliance). Limited-access admin groups can access certain DHCP resources only if their administrative permissions are defined. For information on setting permissions for admin groups, see Chapter 4, Managing Administrators.

**IPv4 DHCP Protocol Overview**

As illustrated in Figure 25.1, when a DHCP client requests an IP address, it sends a DHCPDISCOVER message to the router, which can act as a relay agent. The router forwards the message to the DHCP server. When the DHCP server receives the DHCPDISCOVER message, it determines the network segment to which the client belongs and assigns an IP address. The DHCP server then sends a DHCPOFFER message that includes the IP address and other network configuration information. When the router receives the DHCPOFFER message, it broadcasts the message to the client that sent the DHCPDISCOVER message.

*Figure 25.1 IP Address Allocation Process*

**IPv6 DHCP Protocol Overview**

You can configure NIOS appliances to support DHCP for IPv6 (DHCPv6), the protocol for providing DHCP services for IPv6 networks. The DHCPv6 client-server model is similar to that of IPv4. DHCP clients and servers use a reserved, link-scoped multicast address to exchange DHCP messages. When a DHCP client needs to send messages to a DHCP server that is not attached to the same link, a DHCP relay agent can be used to relay messages between the client and server.

Each IPv6 DHCP server and client has a unique DHCP unique identifier (DUID). DHCP servers use DUIDs to identify clients when providing configuration parameters, and clients use DUIDs to identify the source of the DHCP messages from servers.

As illustrated in Figure 25.2, a DHCP client that needs an IPv6 address sends a Solicit message to the well-known multicast address. DHCPv6 servers then send Advertise messages to the client to indicate that they are available. The client sends a Request message to a specific DHCPv6 server to request IP addresses and configuration parameters. The DHCPv6 server responds with a Reply message that contains the IP addresses and configuration parameters. You can view statistics about the IPv6 messages on the Dashboard.

*Figure 25.2 Client DHCPv6 Configuration Workflow*
Infoblox DHCP servers also supports stateless configuration in which a DHCP client does not need IP addresses, but needs configuration information only. The DHCP client sends an Information-Request packet to obtain configuration information, and the server sends a Reply message with the requested information. For more information, refer to RFC 2462, IPv6 Stateless Address Autoconfiguration.

IPv6 Address Structure

An IPv6 address consists of the following:

- **Global Routing Prefix** — Global routing prefix is a (typically hierarchically-structured) value assigned to a site. For example, an ISP can delegate a prefix to your site, which you can then divide into subnets.
- **Subnet ID** — Subnet ID is an identifier of a link within the site.
- **Interface ID** — Interface Identifier. This portion of the address identifies the interface on the subnet. This is equivalent to the host identifier for IPv4 addresses.

Figure 25.3 IPv6 Address Structure

<table>
<thead>
<tr>
<th>n bits</th>
<th>m bits</th>
<th>128-n-m bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Routing Prefix</td>
<td>Subnet ID</td>
<td>Interface ID</td>
</tr>
</tbody>
</table>

When you enter an IPv6 address in Grid Manager, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:0123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab:0:cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered.

Configuring DHCP Overview

An overview of the complete DHCP configuration process is outlined in the following diagram, illustrating the main steps for preparing a NIOS appliance for use. Note that the process for configuring the DHCP server is the same for IPv4 and IPv6 networks, except that failover associations are not supported in IPv6 networks.
Configuring the Connecting Switch

To ensure that VRRP (Virtual Router Redundancy Protocol) works properly, configure the following settings at the port level for all the connecting switch ports (HA, LAN1, and LAN2):

- Spanning Tree Protocol: Disable. For vendor specific information, search for "HA" in the Infoblox Knowledge Base system at https://support.infoblox.com
- Trunking: Disable
- EtherChannel: Disable
- IGMP Snooping: Disable
- DHCP Snooping: Disable or Enable Trust Interface
- Port Channeling: Disable
- Speed and Duplex settings: Match these settings on both the Infoblox appliance and switch
- Disable other dynamic and proprietary protocols that might interrupt the forwarding of packets

**Note:** You must disable DHCP Snooping to successfully run DHCP services on the Grid. For more information about DHCP services, see About Infoblox DHCP Services.

**Note:** By default, a NIOS appliance automatically negotiates the optimal connection speed and transmission type (full or half duplex) on the physical links between its LAN1 or LAN1 (VLAN), HA, and MGMT ports and the Ethernet ports on the connecting switch. If the two appliances fail to auto-negotiate the optimal settings, see Modifying Ethernet Port Settings for steps you can take to resolve the problem.

Managing DHCP Data

You can configure a NIOS appliance to provide DHCP service for IPv4 and IPv6, and manage both IPv4 and IPv6 objects. When you define DHCP objects, you can track specific information about a network device by defining extensible attributes. Extensible attributes are fields that you define to track properties such as network locations or device models. For more information, see About Extensible Attributes.

About Networks

You can configure DHCP IPv4 and IPv6 properties for the Grid and its members, and then define the IPv4 and IPv6 networks that they serve. All networks, both IPv4 and IPv6, must belong to a network view. The appliance has one default network view and unless you create additional network views, all networks belong to the default view. Note that because network views are mutually exclusive, you can create networks with overlapping IP address spaces in two different network views. For more information, see About Network Views.
Note: The 255.255.255.255 limited broadcast address is reserved. The appliance does not automatically create glue A records for this address. You can however create an NS record without the associated glue records. For more information, see Changing the Interface IP Address.

About Shared Networks

A shared network is a network segment to which you assign two or more subnets. When subnets in a shared network contain IP addresses that are available for dynamic allocation, the addresses are put into a common pool for allocation when client requests arise. When you create a shared network, the DHCP server can assign IP addresses to client requests from any subnet (that resides on the same network interface) in the shared network. For example, when you have networks A, B, and C on the same network interface and you assign them to a shared network, the DHCP server can allocate available IP addresses from any DHCP range within networks A, B, and C even when all the client requests originate from network A. When adding subnets to a shared network, ensure that the subnets are assigned to the same members to avoid DHCP inconsistencies.

Before creating a shared network, you must first create the subnets. For example, you must first create the IPv4 networks 10.32.1.0/24 and 10.32.2.0/24 before designating them to a shared network or create the IPv6 networks 2001:db8:1::/48 and 2001:db8:2::/48 before designating them to a shared network.

After you create a network, you can define their DHCP resources such as DHCP ranges, fixed addresses, reservations, host records, and roaming hosts. IPv4 and IPv6 support most of the same DHCP objects, except that IPv6 does not support reservations.

About DHCP Ranges

A DHCP range is a pool of IP addresses from which the appliance allocates IP addresses. You must add a DHCP address range in your network so the appliance can assign IP addresses to DHCP clients within the specified range. IPv6 DHCP ranges can also contain a range of IPv6 prefixes that it delegates to DHCP clients that request them.

You must assign a DHCP range to a Grid member. Note that you can only assign DHCP ranges to members and networks that are in the same network view. If the server is an independent appliance, you must specify this appliance as the member that serves the DHCP range. In addition, you can also assign IPv4 DHCP ranges to failover associations.

About Exclusion Ranges

You can define an exclusion range within a DHCP range. Creating an exclusion range prevents the appliance from assigning the addresses in the exclusion range to clients. IP addresses in an exclusion range are excluded from the pool of IP addresses. You can use exclusions to split a DHCP range into multiple blocks of ranges. You can also use addresses in the exclusion ranges as static IP addresses for network devices such as legacy printers that do not support DHCP. An exclusion in a range can help prevent address conflicts between statically configured devices and dynamically configured devices.

About Fixed Addresses

You can configure fixed addresses for network devices, such as routers and printers, that are not frequently moved from network to network. By creating fixed addresses for network devices, clients can reliably reach them by their domain names. Some network devices, such as web or FTP servers, can benefit from having fixed addresses for this reason. In IPv4 networks, you can also reserve an IP address that is not part of a DHCP range by defining a reservation. For information about creating reservations, see Configuring IPv4 Reservations.

About Hosts

Infoblox hosts are data objects that contain DNS, DHCP, and IPAM data of the assigned addresses. You can assign multiple IPv4 and IPv6 addresses to a host. When you create a host, you are specifying the name-to-address and address-to-name mappings for the IP addresses that you assign to the host. For information about Infoblox hosts, see About Host Records.

DHCP Configuration Checklists

After you complete the appliance configuration for each member in the Grid, as described in Chapter 8, Managing Appliance Operations, you can configure DHCP services.

The following checklist includes the major steps for configuring DHCP service for IPv4:

<table>
<thead>
<tr>
<th>Step</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 25.1 IPv4 DHCP Configuration Checklist
Configure DHCP properties for the Grid and members.

- Configuring IPv4 DHCP Properties
- Chapter 21, Configuring DNS Updates
- Configuring DHCP IPv4 and IPv6 Common Properties
- Configuring the Lease Logging Member

Decide if you want to configure a DHCP failover association.

- Configuring Failover Associations

Configure networks based on your network requirements and decide if you want to override the Grid or member DHCP configuration for the networks.

- Configuring IPv4 Networks
- Configuring IPv4 Shared Networks

Decide if you want to configure fixed addresses and reservations, and whether to override the Configuring IPv4 Reservations upper level DHCP properties for the fixed addresses and reservations.

- Configuring IPv4 Fixed Addresses
- Configuring IPv4 Reservations

Define DHCP ranges and decide whether to override the upper level DHCP properties for the ranges.

- Configuring IPv6 Address Ranges

Enable DHCP services on the member.

- Starting DHCP Services on a Member

The following checklist includes the major steps for configuring DHCP service for IPv6:

**Table 25.2 IPv6 DHCP Configuration Checklist**

<table>
<thead>
<tr>
<th>Step</th>
<th>For more information</th>
</tr>
</thead>
</table>
| Configure DHCP properties for the Grid and members. | • Configuring DHCPv6 Properties  
• Chapter 21, Configuring DDNS Updates  
• Configuring DHCP IPv4 and IPv6 Common Properties  
• Configuring the Lease Logging Member |
| Configure networks based on your network requirements and decide if you want to override the Grid or member DHCP configuration for the networks. | • Configuring IPv6 Networks  
• About IPv6 Shared Networks |
| Decide if you want to configure fixed addresses and reservations, and whether to override the upper level DHCP properties for the fixed addresses and reservations. | • Configuring IPv6 Fixed Addresses |
| Define DHCP ranges and decide whether to override the upper level DHCP properties for the ranges. | • Configuring IPv6 Address Ranges |
| Enable DHCP services on the member. | • Starting DHCP Services on a Member |

**About DHCP Inheritance**

When you configure DHCP properties for the Grid, members, networks, shared networks, DHCP ranges, fixed addresses, reservations, host addresses, and roaming hosts, the appliance applies the configured properties hierarchically. In addition, IPv4 DHCP objects inherit IPv4 specific properties and IPv6 objects inherit IPv6 specific properties. For example, when you set DHCP IPv4 properties for the Grid, all DHCP IPv4 objects inherit the properties from the Grid unless you override them at a specific level, and the same applies for IPv6 properties and objects. Properties set at the member level override Grid-level settings and apply to the objects within the network. Properties set for a DHCP range override those set at higher levels. You can also set specific properties that apply only to fixed addresses, reservations, host addresses, and roaming hosts. Figure 25.4 illustrates some inheritance scenarios that can occur in a Grid. As shown in the figure, the authoritative server configuration set for the Grid is inherited by the members. Since Member 1 has no overrides and Member 2 overrides the authoritative server configuration, they have different DHCP configurations. Grid Manager applies DHCP properties hierarchically from the Grid down. Therefore, a DHCP object below the member level can inherit DHCP properties with multiple values from multiple sources. In Figure 25.4, network 10.1.1.0/24 inherits multiple values (True and False) from the members for the authoritative server configuration. The shared network, which includes 10.1.1.0/24, inherits DHCP properties from both members. For DHCP range 10.1.1.11 - 10.1.1.50, since Member 1 is the assigned member, it inherits properties from Member 1 and the network. The fixed address 10.1.1.2 overrides the BOOTP settings and inherits the authoritative server configuration from both.
When a DHCP property contains inherited values from different sources, the appliance displays the corresponding information when you create or modify an object. Based on the information provided, you can then decide whether to override or keep the inherited values. You must have read/write permissions to the DHCP resources to override inherited values. You can only view inherited values and paths if you have read-only permissions.

### Overriding DHCP Properties

DHCP properties configured at the Grid level apply to the entire Grid. You can choose to keep the inherited properties or override them when you configure the properties for a member, network, shared network, DHCP range, fixed address, host address, or roaming host. For example, you can override the values of DHCP properties inherited from a member and enter unique values for a network that is configured for DHCP.

To override an inherited value:

1. In a wizard or editor, click **Override** next to a property to enable the configuration. The **Override** button changes to **Inherit**.
2. Enter a new value to override the inherited value.

### Viewing Inherited Values

When you configure DHCP properties that contain inherited values, the appliance displays the information based on the inheritance sources. The following table summarizes what the appliance can display:

<table>
<thead>
<tr>
<th>When you see…</th>
<th>it means…</th>
<th>For details, see…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherited From <code>&lt;object&gt;</code></td>
<td>the DHCP property has a definite value from an inheritance source.</td>
<td><strong>Simple Inheritance</strong></td>
</tr>
<tr>
<td>Inherited From Upper Level</td>
<td>the appliance cannot determine the inherited value or inheritance source for the DHCP property.</td>
<td><strong>Unknown Inheritance</strong></td>
</tr>
<tr>
<td>Inherited From Multiple</td>
<td>the DHCP property has the same value that it inherits from multiple sources.</td>
<td><strong>Multiple Inheritance</strong></td>
</tr>
<tr>
<td>Settings Inherited from Multiple Ancestors, View Multiple Inheritance Scenarios</td>
<td>the DHCP property has multiple values that it inherits from multiple sources, and you can view the values and their corresponding sources by clicking the View Multiple Inheritance Scenarios link.</td>
<td><strong>Multiple Inheritance</strong></td>
</tr>
</tbody>
</table>
Simple Inheritance

When a DHCP property has an inherited value from a specific source, the appliance displays the value. It also displays Inherited From <object> (where <object> can be the Grid, member, network, shared network, or DHCP range) to indicate the source from which the value is inherited. For example, when you set DHCP properties at the Grid level and do not override the properties at any level, the members, networks, shared networks, DHCP ranges, fixed addresses, reservations, host addresses, and roaming hosts inherit these properties from the Grid. The appliance displays the property value and Inherited From Grid Infoblox for each configured DHCP property, as shown in Figure 25.5.

Figure 25.5 Simple Inheritance

Unknown Inheritance

In some cases, DHCP properties may not have definite inherited values and inheritance sources. The following are examples of unknown inheritance:

- The appliance cannot determine the inheritance sources of the DHCP properties in a template until you use the template to create an object.
- When a network or a DHCP range does not have an assigned member, it does not have a clear definition of an inheritance source because a network or a DHCP range inherits properties from a member.
- When individual networks in a shared network do not have member assignments, the shared network has unknown inheritance because the shared network inherits DHCP properties from a member and its networks.
- All roaming hosts have unknown inheritance because the DHCP properties can be inherited from different DHCP ranges within a network view.

In cases where the source of the inheritance is unknown, the appliance displays Inherited From Upper Level as the inheritance source. As shown in Figure 25.6, network 10.1.1.0 has unknown lease time value because it does not have any assigned member.

Figure 25.6 Unknown Inheritance

Multiple Inheritance

As illustrated in Figure 25.7, a network can have multiple inherited values and inheritance sources for DHCP properties when it is served by multiple members. When an object inherits a DHCP property from different sources, the property value can be the same from all sources or it can be different. When the value is the same, the appliance displays the value in the property field. When there are multiple values inherited from multiple paths, the appliance displays the information to indicate so.

In a Grid, when two members serve the same network, the network inherits DHCP properties from both associated members. If both members have the same configured DHCP property, the network inherits the same value from both members. For example, when DHCP network 10.1.1.0
has two associated members and both members have the lease time set for 20 hours, the appliance displays the lease time value and **Inherited From Multiple** to indicate the value is inherited from multiple sources, as shown in *Figure 25.7*. *Figure 25.7 Multiple Inherited Paths with the Same Inherited Value*

In the same Grid with the two members serving the same network, the network inherits different values for the same properties if you override the Grid configuration on one member but not on the other. For example, you can configure different PXE lease times for the members and configure a member as an authoritative DHCP server for the domain and the other not. In this case, the appliance displays **Settings inherited from multiple ancestors** and provides a **View Multiple Inheritance Scenarios** link so you can view the inherited values and paths, as shown in *Figure 25.8*. *Figure 25.8 Multiple Inheritance Sources with Multiple Values*

For example, to view the multiple inherited values of the **Authoritative** field, click **View Multiple Inheritance Scenarios**, and the **Multiple Inheritance Viewer** displays the inherited values from the two members. Since member1.foo.net does not have a configured value for this field, the viewer displays **Not Set**, as shown in *Figure 25.10*. You can use this information to determine whether you want to keep the inherited values or configure new ones. *Figure 25.9 Multiple Inheritance Viewer*

Another scenario of multiple inherited levels is when you have multiple DHCP properties that can inherit the same or multiple values from different sources. For example, when you configure multiple DHCP custom options, each of the options can inherit the same or multiple values from multiple paths. You can override the inherited options and configure new ones at a specific level other than the Grid level. Though these options are grouped under **DHCP Custom Options**, the appliance treats each of them as a separate property. The appliance groups the inherited options at the top, as shown in *Figure 25.10*. You can override these options but you cannot delete them. For multiple values inherited from multiple sources, you can view the values in the **Multiple Inheritance Viewer** by clicking **View Inheritance**, as shown in *Figure 25.11*. *Figure 25.10 DHCP Custom Options with Multiple Inheritance Sources*
When you configure email notification for the Grid or Grid member from the **Data Management** tab -> **Grid** tab, the email address you enter there is inherited by the DHCP configuration for the Grid, members, networks, and DHCP ranges unless you override it at a specific level. The appliance uses this email address to send notification for a DHCP range when the DHCP usage crosses either the effective watermark threshold. For information, see **Configuring Thresholds for DHCP Ranges**.

A network container inherits DHCP options from its parent and grandparent network containers. A network container does not inherit DHCP options defined at the Grid or member level.

Note the following about the DHCP option inheritance:

- For networks and shared networks, you can override an inherited DHCP option defined at the Grid or Member level.
- A shared network without a parent network container continues to inherit DHCP options from its parent Grid or member. The parent object is derived from the first network within the shared network.
- A network inherits DHCP option from its parent object. For example, if a network has a parent network container parent and parent shared network parent, if a DHCP option is overridden on the shared network, then this overridden value gets inherited. If the DHCP option is overridden on a network container, then this overridden value gets inherited. Otherwise, the network continues to inherit from its parent Grid or member.

### About Network Views

A network view is a single routing domain with its own networks and shared networks. A network view can contain both IPv4 and IPv6 networks. All networks must belong to a network view.

You can manage the networks in one network view independently of the other network views. Changes in one network view are not reflected in other network views. Because network views are mutually exclusive, the networks in each view can have overlapping address spaces with multiple duplicate IP addresses without impacting network integrity.

For example, two corporations, Corp 100 and Corp 200, merge. They each have their own networks and DNS domains. They also have their own private IP address spaces in the 10.0.0.0/24 network. Both corporations have DHCP and DNS servers, and use dynamic DNS updates. The DHCP servers of each corporation serve IP addresses for networks in their respective corporations. The DHCP clients in each corporation update DNS zones within their DNS domains.

They plan to migrate the networks and hosts in Corp 200 to the Corp 100 address space and the corpxyz.com domain. To support both networks in the meantime and to facilitate the migration, you can configure an Infoblox Grid to centrally manage the networks and domains of both corporations. As shown in **Figure 25.12**, you can configure network views for each corporation and manage their networks independently of the other. Member 1 serves DNS and DHCP to Corp 100. The networks of Corp 100 are contained in the corp 100 network view, which is associated with both the internal and external DNS views of the corpxyz.com domain. Member 2 serves DNS and DHCP to Corp 200. The networks of Corp 200 are in the corp 200 network view, which is associated with both the internal and external DNS views of the corp200.com domain. The two corporations have one overlapping network, 10.1.1.0/24.

**Figure 25.12 Two Network Views Managed by a Grid**
A Grid member can serve one network view only, but a network view can be served by multiple Grid members. DHCP failover associations must be defined within a single network view, and both the primary and secondary peer must serve the same network view.

The NIOS appliance provides one default network view. You can rename the default view and change its settings, but you cannot delete it. There must always be at least one network view in the appliance. If you do not need to manage overlapping IP address spaces in your organization, you can use the system-defined network view for all your networks. You do not need to create additional network views. But if there are overlapping IP address spaces and you need more than one network view, you can create up to 1000 network views.

Each network view must be associated with at least one DNS view. The default network view is always associated with the default DNS view, which also cannot be deleted. When you create a network view, the appliance automatically creates a corresponding DNS view with the same name as the network view, but with “default” prepended to the name. You can then rename that system-defined DNS view, but you cannot delete it.

A network view can be associated with multiple DNS views (as shown in Figure 25.12), but a DNS view cannot be associated with more than one network view. Each network view must be associated with a unique set of DNS views.

You can initiate a network discovery in only one network view at a time. When you run a discovery task, the appliance sends updates to all DNS views associated with the network view. (For information about network discoveries, see Chapter 14, IP Discovery and vDiscovery.)

Adding Network Views

All networks must belong to a network view. You can use the default network view on the appliance and create additional network views, as needed. If you plan to enable DDNS (dynamic DNS) updates on any of the networks, DHCP ranges and fixed addresses in the network view, you must set parameters that specify which DNS view is updated for each network view.

Note: If there are more than 20 network views, the appliance lists the available network views in the Network View Selector dialog box. If there are 20 or less than 20 network views, the appliance displays them in the drop-down list.

To create a network view:

1. From the Administration tab, select the Network Views tab, and then click the Add icon.
2. In the Network View wizard, do the following:
   - Name: Enter the name of the network view.
   - Comment: Enter useful information about the network view.

The Cloud section displays if the Cloud Network Automation license is installed on the Grid Master. For information, see Deploying Cloud Network Automation.

Delegate authority from the Grid Master

- **Delegate To**: This field indicates whether the authority for the network view you want to create has already been delegated to a Cloud Platform Appliance. Click Select to choose the Cloud Platform Appliance to which you want to delegate authority. The **Me**
member Selector displays only Cloud Platform Appliances in the Grid. Click the member, and Grid Manager displays the member name next to this field. This cloud member now assumes authority for this network view, and the Grid Master does not have authority any more. You can also click Clear to remove authority delegation from the selected Cloud Platform Appliance and return authority back to the Grid Master.

Restricting synchronization of network views

- **Disable sync to MGM**: Select this check box to disable synchronization. This will restrict the synchronization of all objects that are associated with the network view. This check box is available only on the managed Grid when it remains joined with the Multi-Grid Master.

3. Click Next to enter values for required extensible attributes or add optional extensible attributes for the network view. For information, see About Extensible Attributes.

4. Click Next, and then save the configuration or select:

**Configure DDNS Properties**: Configure the DNS zones that are associated with the network view to receive DDNS updates. When you select this option, the Configure DDNS Properties dialog box appears. The appliance saves the network view entry before it opens the Configure DDNS Properties dialog box. For information, see Configuring DDNS Updates.

Modifying Network Views

1. From the Administration tab, select the NetworkViews tab -> network_view check box, and then click the Edit icon.
2. The NetworkView editor provides the following tabs from which you can edit data:

   - **General**: You can modify Name and Comments in this tab. When the Cloud Network Automation license is installed on the Grid Master, Grid Manager displays the following in the Cloud section:
     - **Cloud Usage**: This field indicates whether this object is associated with any specific cloud extensible attributes or within a scope of delegation. It can be one of the following:
       - **Cloud from adapter**: Indicates that this object has been created by a cloud adapter and it may or may not be within a scope of delegation at the moment.
       - **Cloud from delegation**: Indicates that this object is within the scope of delegation or the object itself defines a scope of authority delegation, and it is not created by a cloud adapter.
     - **Used by cloud**: Indicates that this network or network container is associated with the extensible attribute Is External or Is Shared and the value is set to True, which implies the network is a private or shared network managed by the CMP, and it is not Cloud from adapter or Cloud from delegation.
     - **Non-cloud**: The object is a regular NIOS object and is not within the scope of any authority delegation nor is it associated with any of these extensible attributes: Cloud API Owned, Is External or Is Shared. NIOS admin users can modify this object based on their permissions.

   - **Owned By**: A cloud object can be owned by the Grid Master or the cloud adapter. When the object is created by the Cloud Platform member, this shows Grid. If the object is created by the cloud adapter, this shows Adapter.

   - **Delegated To**: This tells you whether a cloud object has been delegated to a Cloud Platform Appliance or not. If the cloud object has a parent object and the parent has been delegated, this field shows the parent delegation and you cannot modify the field.

   - **Restricting synchronization of network views**

   - **Disable sync to MGM**: Select this check box to disable synchronization. This will restrict the synchronization of all objects that are associated with the selected network view. This check box is available only on the managed Grid when it remains joined with the Multi-Grid Master.

3. **Members**: This tab displays the members that provide DHCP services for the networks in this network view. You cannot modify information in this tab. It displays the following:

   - **Name**: The name of the DHCP member.
   - **IP Address**: The IP address of the DHCP member.
   - **Failover Association**: The name of the failover association to which the DHCP member belongs. If there are multiple failover associations, only the first one is displayed.
   - **Comment**: The information that you entered for the DHCP member.

   You can sort the information in the table by column. You can also print and export the information.

4. **Extensible Attributes**: Add and delete extensible attributes that are associated with a specific network view. You can also modify the values of extensible attributes. For information, see About Extensible Attributes.

5. **Permissions**: This tab displays only if you belong to a superuser admin group. For information, see Administrative Permissions for DHCP Resources.

Deleting Network Views

You can delete any network view, except for the default network view. You can delete a network view that has only one DNS view associated with it. You cannot delete a network view that has more than one DNS view associated with it. When you delete a network view, the appliance deletes
all the networks and records within the network view.

To delete a network view:

1. From the Administration tab, select the Network Views tab -> network_view check box, and then click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes.

The appliance removes the network view and its associated DNS views. You can restore the network view from the Recycle Bin, if enabled. If you restore a network view, the appliance restores the associated DNS views as well. For information about the Recycle Bin, see Using the Recycle Bin.

Chapter 26 Configuring DHCP Properties

This chapter explains how to configure DHCP IPv4 and IPv6 properties. It contains the following sections:

- Configuring IPv4 DHCP Properties
- Configuring General IPv4 DHCP Properties
  - Specifying Authoritative
  - Defining Lease Times
  - Configuring General IPv4 Properties
  - Configuring Fixed Addresses without Restarting DHCP Service
- Configuring Ping Settings
- Configuring DHCP Lease Management
- Ignoring DHCP Client Identifiers
- Configuring IPv4 BOOTP and PXE Properties
- About IPv4 DHCP Options
  - DHCP Option Data Types
  - Configuring IPv4 DHCP Options
  - Defining IPv4 DHCP Options
  - Defining IPv4 Option Spaces
  - Configuring Custom DHCP Options
  - Applying DHCP Options
  - Configuration Example: Defining a Custom Option
  - Defining Option 60 Match Rules
  - About the DHCP Relay Agent Option (Option 82)
- Configuring Thresholds for DHCP Ranges
- Configuring DHCPv6 Properties
  - Defining General IPv6 Properties
- About DHCPv6 Options
  - Configuring DHCPv6 Options
  - Defining IPv6 Option Spaces
  - Configuring Custom IPv6 DHCP Options
  - Applying DHCPv6 Options
- Configuring DHCP IPv4 and IPv6 Common Properties
  - Configuring UTF-8 Encoding for Hostnames
  - Associating Networks with Zones
  - Keeping Leases in Deleted IPv4 and IPv6 Networks and Ranges
  - Configuring Fixed Address Leases For Display
  - Scavenging Leases
  - DHCPv6 Lease Affinity
- Configuring DHCP Logging
  - Configuring the Lease Logging Member
- About IF-MAP
  - Configuring a Grid to Support IF-MAP
  - Validating the IF-MAP Server Certificate
  - Configuring Members as IF-MAP Clients
  - Creating IF-MAP Client Certificates
  - Overriding IF-MAP Publishing Settings
  - Deleting Data from the IF-MAP Server
- Starting DHCP Services on a Member
- Viewing DHCP Member Status
  - Viewing DHCP Configuration Files

About DHCP Properties

When you configure a NIOS appliance to function as a DHCP server, you can set DHCP properties that control how the appliance operates and enable DHCP service for IPv4 and IPv6.

You can also specify configuration information the appliance includes in its IPv4 and IPv6 DHCP messages. When a DHCP server assigns an IP address to a client, it can include information the client needs to connect to the network and communicate with other hosts and devices on the network. You can set these properties at the Grid level and override them for a member, network, shared network, DHCP range, fixed address,
IPv4 reservation, host address, or roaming host. When you configure a DHCP object that has inherited DHCP properties, you can either keep the inherited properties or override them. The appliance displays the inherited values and the levels from which the DHCP properties are inherited. For information, see About DHCP Inheritance.

Configuring General IPv4 DHCP Properties

When you configure general IPv4 DHCP properties at the Grid level, the configuration applies to the entire Grid. Though you can set DHCP properties at the Grid level, you can enable DHCP services at the member level only. Infoblox recommends that you configure the DHCP properties before you enable DHCP on the appliance. Depending on the properties, you can override some of them for the members, networks, DHCP ranges, fixed addresses, reservations, host addresses, and roaming hosts. To override an inherited DHCP property, click Override next to the property to enable the configuration.

Specifying Authoritative

Only authoritative DHCP servers can send clients DHCPNAK messages when they request invalid IP addresses. For example, a client moves to a new subnet and broadcasts a DHCPREQUEST message for its old IP address. An authoritative DHCP server responds with a DHCPNAK, causing the client to move to the INIT state and to send a DHCPDISCOVER message for a new IP address. Authoritative servers also respond to DHCPINFORM messages from clients that receive their IP addresses from the DHCP server and require additional options after the initial leases have been granted.

Defining Lease Times

When you configure DHCP general properties, you can specify the length of time the DHCP server leases an IP address to a client. The default on the appliance is 12 hours, and you can change this default according to your network requirements. There are a number of factors to consider when setting the lease time for IP addresses, such as the types of resources and clients on the network, and impact to traffic and performance. With NIOS appliances, you can set lease times at different levels, based on these factors. You can also select the Unlimited Lease Time check box to grant unlimited lease time to IP addresses.

WARNING: Inadvertently selecting the Unlimited Lease Time check box could cause a network outage when the address range runs out of IP addresses.

You can set a default lease time at the Grid level and then override this setting for specific members, network containers, networks, IP address ranges or fixed addresses when appropriate.

Configuring General IPv4 Properties

To configure general IPv4 DHCP properties:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the toolbar. Member: From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon. Network: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon. Network Container: From the Data Management tab, select the IPAM tab -> network_container check box, and then click the Edit icon. DHCP Range: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network->addr_range check box, and then click the Edit icon. Fixed Address: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network->fixed_address check box, and then click the Edit icon. Reservation: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network->reservation check box, and then click the Edit icon.

2. In the DHCP Properties editor of a Grid or member, select the General Basic tab. For all other objects, click Toggle Advanced Mode if the editor is in basic mode. When the additional tabs appear, select the IPv4 DHCP Options Advanced tab.

3. Complete the following:
   - **Authoritative**: Select DHCP server is authoritative to set the DHCP server as authoritative for the domain. This can be set for the Grid, member, network container, network and range.
   - **Lease Time**: Enter the lease time and select the time unit from the drop-down list. The default is 12 hours.
     - **Unlimited Lease Time**: Select this option to set an infinite lease time for all IP addresses.

WARNING: Inadvertently selecting the Unlimited Lease Time check box could cause a network outage when the address range runs out of IP addresses.

To set all other properties for a Grid or member, toggle to the advanced mode and select the General Advanced tab to complete the following:

- **Ignore Optionlist**: Select Ignore optionlist requested by client and return all defined options if you want the appliance to
ignore the requested list of options in the DHCPREQUEST messages it receives from DHCP clients, and to include all the configured options in the DHCPACK and DHCPOFFER messages it sends back to the clients.

- **LEASEQUERY**: Select **Allow LEASEQUERY** to enable the DHCP server to respond to DHCPLEASEQUERY messages.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

**Configuring Fixed Addresses without Restarting DHCP Service**

When you configure or modify a fixed address, a DHCP service restart is required by default in order for the new configuration to take effect. You can override this default behavior by enabling the appliance to take immediate action when you configure or modify a fixed address outside a DHCP range without restarting DHCP service. You can enable this feature at the Grid or member level. Note that when you enable this feature, you cannot use the CLI command `set dhcp_expert_mode`.

**Note**: Enabling this feature might have a significant performance impact on your appliance, depending on the number of fixed addresses you have configured.

For Cloud Network Automation deployment, this feature is automatically enabled on the Cloud Platform Appliance that has a valid Cloud Platform license installed. For information about Cloud Network Automation, see [Deploying Cloud Network Automation](#). To enable immediate fixed address configuration:

1. **Grid**: From the **Data Management** tab, select the **DHCP** tab, and then click **Grid DHCP Properties** from the Toolbar.
2. **Member**: From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box, and then click the **Edit** icon.
3. In the **DHCP Properties editor**, click **Toggle Advanced Mode** if the editor is in basic mode. When the additional tabs appear, click the **General** tab -> **Advanced** tab and complete the following:
   - **Immediate FA Configuration**: Select this check box to enable the new configuration immediately without restarting DHCP service when you modify or delete a fixed address.
4. Save the configuration and restart DHCP service.

**Configuring Ping Settings**

When a DHCP client first tries to connect to a network, it broadcasts its request for an IP address. When the appliance receives such a request, it checks its record of assigned IP addresses and leases. Because there are a limited number of IP addresses available, the appliance reassigns IP addresses whose leases might have expired. Therefore, once the appliance selects a candidate IP address for lease, it sends an ICMP echo request (or ping) to the IP address to verify that it is not in use. If the appliance receives a response, this indicates that the IP address is still in use. Note that the lease status for this IP address is **Abandoned**. The appliance then selects another candidate IP address and sends it a ping. The appliance continues this process until it finds an IP address that does not respond to the ping. The appliance then sends a DHCPOFFER message with the unused IP address to the DHCP client.

*Figure 26.1 Ping Overview*
By default, the appliance pings the candidate IP address once and waits one second for the response. You can change these default settings to better suit your environment. Though you can increase the ping or timeout value to accommodate delays caused by problems in the network, increasing any of these values increases the delay a client experiences when acquiring a lease. You can also disable the appliance from sending pings by changing the number of pings to 0.

You can define ping settings for an entire Grid, and when necessary, define different ping settings for a member. Settings at the member level override settings at the Grid level.

To configure ping settings:

1. **Grid**: From the **Data Management** tab, select the **DHCP** tab, and then click **Grid DHCP Properties** from the Toolbar.

2. **Member**: From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **Members** -> **member** check box, and then click the **Edit** icon.

3. In the **DHCP Properties** editor, click **Toggle Advanced Mode** if the editor is in basic mode. When the additional tabs appear, click the **General** tab -> **Advanced** tab and complete the following:
   - **Number of Ping Requests**: Enter the number of pings the appliance sends to an IP address to verify that it is not in use. The range is 0 to 10, inclusive. Enter 0 to disable DHCP pings.
   - **Ping Timeout**: Select the ping timeout value from the drop-down list.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Configuring DHCP Lease Management

When setting up DHCP properties, you can configure how the appliance handles lease management. For example, when a DHCP client moves from one network to another, the DHCP lease granted by the DHCP server in the previous network remains associated with the network device until the lease expires. When this happens to multiple clients, the address range could run out of IP addresses, thus preventing other clients from retrieving an IP address. To avoid this, you can configure the DHCP server to release a lease when a client moves out of the network. Note that this is valid only if the client has included the client ID while requesting a lease. For example, a DHCP IPv4 client has included the client ID while requesting a lease from network A. This client then moves from network A to B. The DHCP server immediately releases the lease for reuse by another client on network A, based on the client ID. If the client does not include the client ID in the request, the lease on network A remains active until the lease expires.

You can also enable one-lease-per-client to ensure that each DHCP IPv4 client receives only one lease at any given time. When you enable one-lease-per-client and a DHCP client sends a DHCPREQUEST for a particular lease, the appliance releases other leases that the client holds, on the interface that the client is currently using.

Enabling one-lease-per-client is useful when you want to control the number of leases on your subnets and ensure that each DHCP client receives only one lease at a time. Typically, you enable one-lease-per-client for a DHCP client that moves around a lot within different subnets and uses long leases.

Note that this feature supports only DHCP IPv4 clients. When you configure lease management at the Grid level, all members inherit the setting. You can override the Grid setting for each member.
Note: One-lease-per-client enables a single lease per client on a per member basis, not on a Grid wide basis. Lease information is not replicated among members. Note that you must restart the DHCP service for the changes to take effect.

To configure DHCP lease management:

1. **Grid:** From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar. 
   - **Member:** From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.
   - **Standalone DHCP:** From the Data Management tab, select the DHCP tab, expand the Toolbar and click System DHCP Properties.
   - **Advanced DHCP:** From the Data Management tab, select the DHCP tab -> Advanced tab and select the respective radio button under Multiiple Lease Management:
     - **Release leases for clients with Client IDs:** Select this option to release only those leases that have a client ID when the clients move from one network to another before the leases expire. This is selected by default. The DHCP server does not release leases that do not have a client ID.
     - **Retain leases for clients with Client IDs:** Select this option to retain all the leases the client holds. The DHCP server retains all the leases either with or without a client ID. The amount of time taken by the DHCP server to find a lease for a client might increase if you use this option when the pools are almost full. Choosing this option might also increase the amount of active leases in the pools when the client moves from one network to another.
     - **Allow only one lease per client:** Select this option to enable one-lease-per-client per Grid member. This is valid for leases both with and without client IDs.

2. Save the configuration and click **Restart** if it appears at the top of the screen.

**Ignoring DHCP Client Identifiers**

You can set the DHCP server to ignore the UID (unique client identifier) and MAC address (hardware address) of a DHCP client when it places a request to the DHCP server for a new lease. When you configure the appliance to ignore the MAC address of a DHCP client, you can specify the list of MAC addresses. You can enter up to 10 MAC addresses to be ignored. The appliance ignores all the MAC addresses if you do not specify any MAC addresses. If the Ignore Hardware Address option is enabled and a DHCP client makes a request without a client UID for a new lease, then the appliance drops this request. This option is disabled by default. When you enable "Ignore DHCP Client ID" and a DHCP client sends a DHCPREQUEST for a lease, the DHCP server identifies the DHCP client using the physical MAC address of the appliance while the UID is ignored. The DHCP client then allocates an IP address based on the MAC address of the DHCP client. For example, when a DHCP client places a request for a new lease, the DHCP server identifies the DHCP client with the MAC address and allocates the same IP address that was previously allocated for that MAC address. You can define this feature at the Grid level, which is inherited at the member, shared network, IPv4 network and range level. This feature is disabled by default.

**Note:** This feature is applicable only to dynamic leases and does not have any effect on the static lease generated for fixed addresses or roaming hosts.

To ignore the client identifier of DHCP clients:

1. **Grid:** From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar. 
   - **Member:** From the Data Management tab, select the DHCP tab -> and click the Members tab -> member check box -> Edit icon.
   - **Standalone DHCP:** From the Data Management tab, select the DHCP tab, and then click System DHCP Properties.
   - **Shared Network Editor:** From the Data Management tab, select the DHCP tab -> Networks tab -> Shared Networks section -> share d_network check box, and then click the Edit icon.
   - **IPv4 Network Editor:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section ->network check box, and then click the Edit icon.
   - **IPv4 Range Editor:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> click on the network address. Select the IP address range check box, and then click the Edit icon.

2. In the DHCP Properties editor, select the General tab -> Advanced tab (or click Toggle Advanced Mode) and then complete the following:
   - **Accept Client Identifier and MAC Address:** Select this check box to instruct the DHCP server to recognize MAC address and client UID of a DHCP client when it requests for a new lease.
   - **Ignore Client Identifier:** By default, this check box is not selected at the Grid level. Select this check box to ignore the client identifier of a DHCP client while placing a request to the DHCP server for a new lease. The DHCP server will only identify the MAC address and ignores the client identifier. DHCP clients requesting leases with different client UIDs receive the same IP address based on the MAC address. The initial default state is inherited from the Grid level. Click **Override** to modify the inherited setting. To inherit the Grid settings, click **Inherit** at the member, IPv4 network and range, or shared network level.
   - **Ignore MAC Address:** By default, this check box is not selected at the Grid level. Select this check box to ignore MAC address of a DHCP client while placing a request to the DHCP server for a new lease. To override the value that has been inherited from the Grid, click **Override**. Click the Add icon, the appliance adds a row to the table. Click the row and enter the MAC address to be ignored. You can also select a check box and click the Delete icon to delete the MAC address. To inherit the Grid settings, click **Inherit** at the member, IPv4 network and range, or shared network level.

3. Save the configuration and click **Restart** at the top of the screen.
Limitations of the Ignore Client ID Feature on DHCP Failover Associations

- You cannot assign a DHCP range that has the ignore DHCP client ID feature enabled to a DHCP failover association if:
  - one of the members is an external DHCP server in the failover association.
  - one of the members is running a NIOS version earlier than 6.12.
- The DHCP failover association does not work if a DHCP range having multiple inherited values has the ignore DHCP client ID feature enabled on one server and disabled on the other.
- The range assigned to a DHCP failover association and the member (failover peer) must have the same DHCP range setting. The DHCP failover association does not work if a range associated with it does not have the same ignore DHCP client ID setting as the member.

Configuring IPv4 BOOTP and PXE Properties

You can configure the DHCP server to support IPv4 clients that use BOOTP (bootstrap protocol) or that include the TFTP server name option and boot file name option in their DHCPREQUEST messages. You can specify the name or IP address of the boot server and the name of the file the host needs to boot.

In addition, you can configure the DHCP server to support hosts that use PXE (Preboot Execution Environment) to boot remotely from a server. When such a host starts up, it first requests an IP address so it can connect to a server on the network and download the file it needs to boot. After it downloads the file, the host reboots and sends another IP address request. To better manage your IP resources, set a different lease time for PXE boot requests. You can configure the DHCP server to allocate an IP address with a shorter lease time to hosts that send PXE boot requests, so IP addresses are not leased longer than necessary.

Note: When you assign a failover association to serve DHCP ranges and networks, NIOS denies dynamic BOOTP clients by default, regardless of whether you select or deselect the Deny BOOTP Requests option from Grid Manager. However, if the DHCP ranges or networks are assigned to a single DHCP server (not a failover association), NIOS does not automatically deny dynamic BOOTP clients. In this case, you must manually select the Deny BOOTP Requests option through Grid Manager to ensure that NIOS denies BOOTP requests to avoid problems such as receiving two IP addresses for the same network device.

You can configure BOOTP and PXE properties at the Grid level and override them for members, IPv4 network containers, IPv4 networks, DHCP ranges, fixed addresses, and reservations, host addresses, and roaming hosts. You cannot configure BOOTP and PXE properties for IPv6 DHCP objects.

To configure or override BOOTP and PXE properties:

1. **Grid Level:** From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
   - **Member Level:** From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.
   - **Network Level:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.
   - **Network Container:** From the Data Management tab, select the IPAM tab -> network_container check box, and then click the Edit icon.
   - **DHCP Range Level:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network-> addr_range check box, and then click the Edit icon.
   - **Fixed Address Level:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> fixed_address check box, and then click the Edit icon.
   - **Reservation:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> reservation check box, and then click the Edit icon.

2. In the DHCP Properties editor, select the BOOTP/PXE tab and complete the following:
   - **PXE Lease Time:** Click Override and select Enable PXE Lease Time if you want the DHCP server to use a different lease time for PXE clients. You can specify the duration of time it takes a host to connect to a boot server, such as a TFTP server, and download the file it needs to boot. For example, set a longer lease time if the client downloads an OS (operating system) or configuration file, or set a shorter lease time if the client downloads only configuration changes. Enter the lease time for the preboot execution environment for hosts to boot remotely from a server.
   - **Deny BOOTP Requests:** Select this checkbox to disable the BOOTP settings and deny BOOTP boot requests. If you assign DHCP ranges or networks to a single DHCP server (not a failover association), NIOS does not automatically deny dynamic BOOTP clients. In this case, you must select this option to ensure that NIOS denies BOOTP requests to avoid problems such as receiving two IP addresses for the same network device.
   - **Complete the following in the BOOTP Settings section:**
     - **Boot File:** Enter the name of the boot file the client must download.
     - **Next Server:** Enter the IP address or hostname of the boot file server where the boot file is stored. Complete this field if the hosts in your network send requests for the IP address of the boot server. If the TFTP server is the NIOS appliance that is also serving DHCP, enter the IP address of the appliance.
     - **Boot Server:** Enter the name of the server on which the boot file is stored. Clients can request for either the boot server name or IP address. Complete this field if the hosts in your network send requests for the boot server name. If the TFTP server is the appliance that is also serving DHCP, enter the name of the appliance

Note: Enter values in both the **Next Server** and **Boot Server** fields if some hosts on your network require the boot server name and others require the boot server IP address.

3. Save the configuration and click **Restart** if it appears at the top of the screen.
Note that a few characters need manual escaping when you configure a DHCP boot file name, in order to keep the dhcpd.conf file consistent. If you do not use appropriate escape characters, then it might lead to a non working boot file name. The following characters require manual escaping:

- \t \t - Tabulation character
- \r \r - Carriage return
- \n \n - New line
- \b \b - Bell
- \xYY \xYY - YY hex-number (a-f, 0-9)

For example, if you set the 'Boot File' to:

```
\x86\topdir\subdir\file.img'
```

You might need to enter \x and \t as the manual escape characters:

```
'\x86\topdir\subdir\file.img'
```

You can also specify all \ as the manual escape character:

```
'\x86\topdir\subdir\file.img'
```

The above commands result in the underlying dhcpd.conf file:

```
'\x5cx86\x5ctopdir\x5csubdir\x5cfile.img'
```

or

```
'\x5cx86\x5ctopdir\x5csubdir\x5cfile.img'
```

### About IPv4 DHCP Options

DHCP options provide specific configuration and service information to DHCP clients. These options appear as variable-length fields at the end of the DHCP messages that DHCP servers and clients exchange. For example, DHCP option 3 is used to list the available routers in the network of the client and option 6 is used to list the available DNS servers.

An option space is a collection of options. ISC (Internet Systems Consortium) DHCP has five predefined option spaces: dhcp, agent, server, nwip, and fqdn. The NIOS appliance supports only the predefined DHCP option space, which contains the industry standard options as well as additional options you can configure as needed:

- **Predefined options:** These are option codes 1 to 125. They are allocated by the IANA and defined by IETF standards. The DHCP server knows these standard options, and they are predefined on the server. You cannot redefine these options or delete them from the DHCP option space.
- **Custom options:** These are option codes 126 to 254. They are not defined by IETF standards and are available for private use. You can use these option codes to provide configuration or service information that none of the predefined options provide.

You can also create option spaces to define new groups of options. For example, you can create additional option spaces to define vendor specific options, which are encapsulated in option 43. When a DHCP client requests vendor specific options, it makes a request using the vendor identifier set in option 60 and a list of requested vendor specific options (option 43). The DHCP server then responds with the list of replies for the various options encapsulated into option 43.

Note that custom options defined in the DHCP option space are included in the options section of the DHCP messages that DHCP servers and clients exchange. Custom options defined in a user-defined option space are always encapsulated in option 43 in DHCP messages.

You can apply options globally at the Grid level, or more specifically at the member, network, network container, range, host and roaming host levels.

A network inherits DHCP options from its parent object. You can override the inherited DHCP options configured at the Grid or Member level for the networks and shared networks. If a network has a parent network container and parent shared network and if you override the DHCP options on the shared network, then the network inherits the shared network values. If you override the DHCP options at the network container level, then the network inherits the network container values. Otherwise, the network continues to inherit DHCP options from its parent Grid or member. A shared network without a parent network container continues to inherit DHCP options from its parent Grid or member. The parent object is derived from the first network within the shared network. A network container inherits DHCP options from its parent and grandparent network containers. A network container does not inherit DHCP options defined at the Grid or member level.

To override an inherited value, click **Override** next to it and complete the appropriate fields. When you click **Override**, the appliance displays the value inherited from its parent object (if any). If you do not set any value at the higher level, the appliance displays the default DHCP options. The following table lists the default DHCP Options:

<table>
<thead>
<tr>
<th>Table 26:1 Default DHCP Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>IPV4 Common DHCP Options</td>
</tr>
<tr>
<td>Enable PXE Lease Time</td>
</tr>
<tr>
<td>Lease Time</td>
</tr>
<tr>
<td>Routers</td>
</tr>
<tr>
<td>Domain Name</td>
</tr>
<tr>
<td>DNS Servers</td>
</tr>
<tr>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Broadcast Address</td>
</tr>
<tr>
<td>Custom DHCP Options</td>
</tr>
<tr>
<td>Lease Scavenging</td>
</tr>
<tr>
<td>Authoritative (Advanced)</td>
</tr>
<tr>
<td>Lease Deletion (Advanced)</td>
</tr>
<tr>
<td>Ignore Optionlist (Advanced)</td>
</tr>
<tr>
<td>IPv4 DDNS</td>
</tr>
<tr>
<td>Enable DDNS Updates</td>
</tr>
<tr>
<td>DDNS Domain Name</td>
</tr>
<tr>
<td>DDNS Update TTL</td>
</tr>
<tr>
<td>DDNS Update Method</td>
</tr>
<tr>
<td>Generate Hostname</td>
</tr>
<tr>
<td>Fixed Address Updates</td>
</tr>
<tr>
<td>Option 81 Support</td>
</tr>
<tr>
<td>Lease Renewal Update</td>
</tr>
<tr>
<td>IPv4 Threshold Options</td>
</tr>
<tr>
<td>Enable DHCP Thresholds</td>
</tr>
<tr>
<td>High - Trigger</td>
</tr>
<tr>
<td>High - Reset</td>
</tr>
<tr>
<td>Low - Trigger</td>
</tr>
<tr>
<td>Low - Reset</td>
</tr>
<tr>
<td>Enable SNMP Warnings</td>
</tr>
<tr>
<td>Enable Email Warnings</td>
</tr>
<tr>
<td>Email Addresses</td>
</tr>
<tr>
<td>IPv4 BOOTP/PXE</td>
</tr>
<tr>
<td>Enable PXE Lease Time</td>
</tr>
<tr>
<td>Lease Time (Value)</td>
</tr>
<tr>
<td>Deny-BOOTP-Requests</td>
</tr>
<tr>
<td>Boot File</td>
</tr>
<tr>
<td>Next Server</td>
</tr>
<tr>
<td>Boot Server</td>
</tr>
<tr>
<td>IPv6 DHCP Options</td>
</tr>
<tr>
<td>Valid Lifetime</td>
</tr>
<tr>
<td>Preferred Lifetime</td>
</tr>
<tr>
<td>Domain Name</td>
</tr>
<tr>
<td>DNS Servers</td>
</tr>
</tbody>
</table>
Custom DHCP Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lease Deletion</td>
<td>Enabled</td>
</tr>
<tr>
<td>Lease Scavenging</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

IPv6 DDNS Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable DDNS Updates</td>
<td></td>
</tr>
<tr>
<td>DDNS Domain Name</td>
<td></td>
</tr>
<tr>
<td>DDNS Update TTL</td>
<td>0</td>
</tr>
<tr>
<td>DDNS Update Method</td>
<td>Interim</td>
</tr>
<tr>
<td>Generate Hostname</td>
<td>Disabled</td>
</tr>
<tr>
<td>FQDN Support</td>
<td>Disabled</td>
</tr>
<tr>
<td>• DHCP server always updates DNS</td>
<td></td>
</tr>
<tr>
<td>• DHCP server updates DNS if requested by client</td>
<td></td>
</tr>
<tr>
<td>Lease Renewal Update</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

You can also create an option filter the appliance uses to filter address requests by the DHCP options of requesting hosts. The filter instructs the appliance to either grant or deny an address request if the requesting host matches the filter. For information, see Defining Option Filters.

The DHCP option configuration conforms to the following RFCs:

- RFC 2132, DHCP Options and BOOTP Vendor Extension
- RFC 3046, DHCP Relay Agent Information Option. The supported options include option 60 (Client Identifier), 21 (Policy Filter), 22 (Maximum Datagram Reassembly Size), 23 (Default IP Time-to-Live), and 82 (Support for Routed Bridge Encapsulation).
- RFC 3925, Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)
- RFC 2939, Procedures and IANA Guidelines for Definition of New DHCP Options and Message Types

DHCP Option Data Types

Each DHCP option is identified by a name and an option code number, and specifies a data type. The data type for some options is predefined. For example, in the DHCP option space, the data type for option 1: subnet-mask is an IP address. You cannot change the data type for this option. The data type for some options is user-defined and can be in one of the formats shown in Table 26.2.

### Table 26.2 DHCP Option Data Types

<table>
<thead>
<tr>
<th>Data type</th>
<th>Specifies</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>An ASCII text string (the same as the text data type) or a list of hexadecimal characters separated by colons</td>
</tr>
<tr>
<td></td>
<td>Formatting to distinguish an ASCII text string from a hexadecimal string is important. For details, see the following section</td>
</tr>
<tr>
<td>Boolean</td>
<td>A flag with a value of either true or false (or on or off)</td>
</tr>
<tr>
<td>IP address</td>
<td>A single IP address</td>
</tr>
<tr>
<td>Array of IP addresses</td>
<td>A series of IP addresses, separated by commas</td>
</tr>
<tr>
<td></td>
<td>You can optionally include a space after each comma</td>
</tr>
<tr>
<td>Text</td>
<td>An ASCII text string</td>
</tr>
<tr>
<td>8-, 16-, or 32-bit unsigned integer</td>
<td>A numeric range of the following possible values</td>
</tr>
<tr>
<td></td>
<td>8-bit unsigned integer: from 0 to 255</td>
</tr>
<tr>
<td></td>
<td>16-bit unsigned integer: from 0 to 65,535</td>
</tr>
<tr>
<td></td>
<td>32-bit unsigned integer: from 0 to 4,294,967,295</td>
</tr>
</tbody>
</table>
8-, 16-, or 32-bit signed integer

A numeric range of the following possible values

- 8-bit signed integer: from -128 to 127
- 16-bit signed integer: from -32,768 to 32,767
- 32-bit signed integer: from -2,147,483,648 to 2,147,483,647

Domain name

A list of domain names, separated by spaces

When defining a hexadecimal string for a DHCP option (such as option 43, vendor encapsulated options), use only hexadecimal characters (0-9, a-f, or A-F) without spaces and separated by colons. The accepted form for a hexadecimal string, as presented in a regular expression, is 

```
[0-9a-fA-F]{1,2}(:[0-9a-fA-F]{1,2})*
```

Two examples of correctly written hexadecimal strings:

- `aa:de:89:1b:34`
- `1C:8:22:A3` (Note that the DHCP module treats a single hexadecimal character, such as "8" as "08").

A few examples of incorrectly written hexadecimal strings:

- `.bb:45:d2:1f` – Problem: The string erroneously begins with a colon.
- `bb:4 5:d2:1f` – Problem: The string erroneously includes a space between two characters ("4" and "5").
- `bb:45:d2:1g` – Problem: The string erroneously includes a nonhexadecimal character ("g").

The DHCP module treats incorrectly written hexadecimal strings as simple text strings, not hexadecimal strings. If the string appears in quotes, it is a text string.

Configuring IPv4 DHCP Options

To use DHCP options, you can do the following:

- Define basic DHCP options, as described in Defining IPv4 DHCP Options.
- Configure one or more option spaces, as described in the next section Defining IPv4 Option Spaces.
- Define custom options in the predefined DHCP option space or add options to an option space that you configured. For more information, see Configuring Custom DHCP Options.
- Specify values for the options and apply them to the Grid, or to a member, network, range, fixed address, reservation, host, or roaming host. For more information, see Applying DHCP Options.

Defining IPv4 DHCP Options

You can define basic DHCP options that the DHCP server uses to provide configuration information to DHCP clients. The server includes these options in its DHCP messages.

To define DHCP options:

1. Network: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.
   - **Network Container:** From the Data Management tab, select the IPAM tab -> network_container check box, and then click the Edit icon.
   - **DHCP Range:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> DHCP_range check box, and then click the Edit icon.
   - **Fixed Address:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> fixed_address check box, and then click the Edit icon.
   - **Reservation:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> reservation check box, and then click the Edit icon.
   - **Host Address:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> host_record check box, and then click the Edit icon. Select the host IP address, and then click the Edit icon.
   - **Roaming Host:** From the Data Management tab, select the DHCP tab -> Networks tab -> Roaming Hosts -> roaming_host check box, and then click the Edit icon.
2. In the DHCP Properties editor, select the IPv4 DHCP Options tab and complete the following:
   - **Routers:** Click the Add icon. Grid Manager adds a row to the table. In the table, enter the IP address of the router that is connected to the same network as the DHCP client. When configuring this for a template, enter the offset value of the IP address of the router. The DHCP server includes this information in its DHCP OFFER and DHCPACK messages.
   - **DomainName:** Enter the name of the domain for which the Grid serves DHCP data. The DHCP server includes this domain name in Option 15 when it responds with a DHCP OFFER packet to a DHCP DISCOVER packet from a client. If DDNS is enabled on the DHCP server, it combines the host name from the client and this domain name to create the FQDN (fully-qualified domain name) that it uses to update DNS. For information about DDNS, see Chapter 21, Configuring DDNS Updates. When overriding the domain name already set by a parent object, enter the new value for the selected option or use "" to clear the value.
- DNS Servers: Click the Add icon. Grid Manager adds a row to the table. In the table, enter the IP address of the DNS server to which the DHCP client sends name resolution requests. The DHCP server includes this information in the DHCP OFFER and DHCPACK messages.
- Broadcast Address: Enter the broadcast IP address of the network to which the DHCP server is attached. When configuring this for a template, enter the offset value of the broadcast IP address of the network.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

### Defining IPv4 Option Spaces

DHCP members support the DHCP option space by default. You can create additional option spaces to provide additional configuration or service information. Note that custom options defined in a user-defined option space are always encapsulated in option 43 in DHCP messages.

To add a custom option space:

1. From the **Data Management** tab, select the **DHCP** tab -> **Option Spaces** tab.
2. Click the Add icon -> IPv4 Option Space.
3. In the **Option Space** wizard, do the following:
   - **Name**: Enter the name of the option space.
   - **Comment**: Enter useful information about the option space.
   - **Options**: Click the Add icon to add options. For additional information, see the next section, *Configuring Custom DHCP Options*.
4. Save the configuration and click **Restart** if it appears at the top of the screen.

After you create an option space and add options to it, you can apply the options as described in *Applying DHCP Options*.

### Configuring Custom DHCP Options

You can define custom options in the DHCP option space or in an option space that you configured, as follows:

1. From the **Data Management** tab, select the **DHCP** tab -> **Option Spaces** tab.
2. Select either the **DHCP** option space or an IPv4 option space that you configured, and then click the **Edit** icon.
3. In the **Option Space** editor, click the Add icon to add a custom option. In the new row, complete the following:
   - **Name**: Enter the name of the custom DHCP option.
   - **Code**: Select an option code from the drop-down list. Select a number between 126 and 254 if you are adding custom options to the DHCP option space. If you are adding custom options to an IPv4 option space you configured, you can enter a number between 1 and 254.
   - **Type**: Select the option type (such as ip-address, text, boolean, and string as described in *Table 26.2*).
     - For example, to create an option that defines the IP addresses of Solaris root servers, enter the name SrootIP4, select option code 126, and then select the type as ip-address.

   Click the Add icon to add more options.
4. Save the configuration.

### Applying DHCP Options

Some options may apply to all networks and some may apply to specific ranges and even hosts. When you apply an option, you select the object to which the option is applied, such as the Grid member, or network, and then specify a value for the option.

Use the following guidelines when specifying option values:

- Enter **false** or **true** for a Boolean Flag type value.
- Enter an ASCII text string, or enter a series of octets specified in hex, separated by colons.
- Separate multiple values by commas. For example, to enter multiple IP addresses for netbios-name-servers, enter a comma between each IP address.

Here are some examples of option names and correctly formatted values:

<table>
<thead>
<tr>
<th>Option name</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>option 61</td>
<td>MyPC</td>
<td>Double quotes are no longer needed for string type values</td>
</tr>
<tr>
<td>dhcp-client-identifier</td>
<td>43:4c:49:45:54:2d:46:4f:4f</td>
<td>Series of octets specified in hex, separated by colons for a Data-string type value</td>
</tr>
<tr>
<td>netbios-name-servers</td>
<td>10.1.1.5,10.1.1.10</td>
<td>Multiple IP addresses separated by commas</td>
</tr>
<tr>
<td>option-80</td>
<td>ABC123</td>
<td>Custom option number 80 set to the string ABC123.</td>
</tr>
</tbody>
</table>
To apply DHCP options:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.

- **Member**: From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.
- **Network**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.
- **Network Container**: From the Data Management tab, select the IPAM tab -> network_container check box, and then click the Edit icon.
- **DHCP Range**: From the DataManagement tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.
- **Fixed Address**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> fixed_address check box, and then click the Edit icon.
- **Reservation**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> reservation check box, and then click the Edit icon.
- **Host Address**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> host_record check box, and then click the Edit icon.
- **Roaming Host**: From the Data Management tab, select the DHCP tab -> Networks tab -> Roaming Hosts -> roaming_host check box, and then click the Edit icon.

2. In the **DHCP Properties** editor, select the IPv4 DHCP Options and complete the following:
   - The **Custom DHCP Options** section displays two fields. The first field displays Choose option. Click the arrow and select an option from the list. In the second field, enter a value for the selected option. Note that certain options have predefined data types and their values must be entered in a specific format. For information about the data types, see **DHCP Option Data Types**.
   - Click + to add another option, or click - to delete a previously specified option. When overriding an option already set by a parent object, enter the new value for the selected option or use "" to clear the value.
   - Note that if you created an option space as described in **Defining IPv4 Option Spaces**, this section displays a list of option spaces in the first drop-down menu, so you can select the option space of the option you want to define.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

**Configuration Example: Defining a Custom Option**

In this example, you configure two custom options in the DHCP option space, and apply them to a DHCP range in the network 192.168.2.0/24.

Add the custom options to the DHCP options space:

1. From the Data Management tab, select the DHCP tab -> Option Spaces tab.
2. Select the DHCP check box, and click the Edit icon.
3. In the DHCP (Option Space) editor, click the Add icon. In the new row, complete the following:
   - **Name**: Enter tftp-server.
   - **Code**: Enter 150.
   - **Type**: Select array of ip-address.
4. Click the Add icon to add another option. In the new row, complete the following:
   - **Name**: Enter pxe-configfile.
   - **Code**: Enter 209.
   - **Type**: Select text.
5. Click Save & Close.

Enter values for the newly defined custom options and apply them to a DHCP range:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks subtab, and click the 192.168.2.0/24 network.
2. Click the 192.168.2.10 - 100 check box, and then click the Edit icon.
3. In the DHCP Properties editor, select the DHCP tab and complete the following in the Custom DHCP Options section:
   - From the drop-down list of options, select tftp-server (150) array of address. In the second field, enter 192.168.1.2.
   - Click + to add another option.
   - From the drop-down list of options, select pxe-configfile (209) text. In the second field, enter pxe.config, which is the file name of the boot image.
4. Save the configuration and click **Restart** if it appears at the top of the screen.

The member then includes options 150 and 209 in its DHCP messages to clients that are allocated IP addresses from the DHCP range 192.168.2.10 - 100.

**Defining Option 60 Match Rules**

The appliance uses option 60 (vendor-class-identifier) to forward client requests to the DHCP server for services that the clients require. You can define option 60 match rules and filter on these rules. You can set these rules for the Grid and override for a member.

To define option 60 for the Grid or member:
1. **Grid**: From the [Data Management tab](#), select the [DHCP tab](#), and then click [Grid DHCP Properties](#) from the [Toolbar](#).

   **Member**: From the [Data Management tab](#), select the [DHCP tab](#) -> [Members tab](#) -> [Members](#) -> member check box, and then click the [Edit icon](#).

2. In the [DHCP Properties editor](#), click [Toggle Advanced Mode](#) if the editor is in basic mode. When the additional tabs appear, click the [DHCP Options tab](#) -> [Advanced tab](#) and complete the following:

   To override the Grid configuration for a member, click [Override](#) next to the property. Grid Manager hides the Grid configuration. You can then add new values for the member.

   - **Option60 (Vendor Class Identifier) Match Rules**: Click the [Add icon](#) if you want to add a match rule to a vendor class option. The appliance adds a row to the table. Complete the following:
     - **Option Space**: Select an option space from the drop-down list. This field appears only when you have custom option spaces. The appliance uses the default [DHCP option space](#) if you do not have custom option spaces.
     - **Match Value**: Enter the value you want the appliance to use when matching vendor class options.
     - **Is Substring**: Select this check box if the match value is a substring of the option data.
     - **Substring Offset**: Enter the number of characters at which the match value substring starts in the option data. Enter 0 to start at the beginning of the option data, enter 1 for the second position, and so on. For example, when you enter 2 here and have a match value of RAS, the appliance matches the value RAS starting at the third character of the option data.
     - **Substring length**: Enter the length of the match value. For example, if the match value is SUNW, the length is 4.

3. Save the configuration and click [Restart](#) if it appears at the top of the screen.

### About the DHCP Relay Agent Option (Option 82)

A typical relationship between a DHCP client, relay agent, and the NIOS appliance on a network is as follows:

1. A DHCP client broadcasts a DHCPDISCOVER message on its network segment.
2. A DHCP relay agent on that segment receives the message and forwards it as a unicast message to one or more DHCP servers (such as NIOS appliances).
3. If the NIOS appliance accepts the address request, it responds to the relay agent with a DHCPOFFER message. If the appliance denies the request, it does not send any response in case other DHCP servers that might be involved respond instead.
4. The relay agent forwards the response to the client, usually as a broadcast message.

The situation is different for individual hosts connecting to the Internet through an [ISP](#), usually over a circuit-switched data network.

1. A host connects to its ISP’s circuit access concentration point, authenticates itself, and requests an IP address.
2. The circuit access unit relays the address request to a DHCP server, which responds with a DHCPoffer message.

To avoid broadcasting the DHCPoffer over the network segment on which the host made the request, the relay agent sends the response directly to the host over the established circuit.

Option 82 assists the agent in forwarding address assignments across the proper circuit. When a relay agent receives a DHCPDISCOVER message, it can add one or two agent IDs in the DHCP option 82 suboption fields to the message.

The two relay agent IDs are:

- **Circuit ID**: This identifies the circuit between the remote host and the relay agent. For example, the identifier can be the ingress interface number of the circuit access unit (perhaps concatenated with the unit ID number and slot number). The circuit ID can also be an ATM virtual circuit ID or cable data virtual circuit ID.
- **Remote ID**: This identifies the remote host. The ID can be the caller ID telephone number for a dial-up connection, a user name for logging in to the ISP, a modem ID, and so on. Because the remote ID is defined on the relay agent, which is presumed to have a trusted relationship with the DHCP server, and not on the untrusted DHCP client, the remote ID is also presumably a trusted identifier.

**Note**: For information about the relay agent option, refer to [RFC3046, DHCP Relay Agent Information Option](#).

### Defining Logging Format for DHCP Option 82

When you define the circuit ID or remote ID of the relay agent as a host identifier, you can choose the logging format Grid Manager uses to display the IDs in the detailed lease information panel. For information about viewing lease information, see [Viewing Detailed Lease Information](#).

To define logging format for the agent ID, circuit ID and remote ID, complete the following:

1. **Grid**: From the [Data Management tab](#), select the [DHCP tab](#), and then click [Grid DHCP Properties](#) from the [Toolbar](#).
   **Independent Appliance**: From the [Data Management tab](#), select the [DHCP tab](#), and then click [System DHCP Properties](#).
2. In the [Grid DHCP Properties](#) or [System DHCP Properties](#) editor, select the [General tab](#) -> [Advanced tab](#).
3. Select one of the following for **Logging format for Option82**: 
   - **Hexadecimal**: When you select this, Grid Manager displays the agent ID, circuit ID, and remote ID in hexadecimal format in the detailed lease information. This is the default format.
   - **Plaintext**: When you select this, Grid Manager displays the agent ID, circuit ID, and remote ID in plain text in the detailed lease information.

**Note**: You cannot override this Grid setting at the member level. Also, changing the logging format requires a DHCP service restart.

### Configuring IPv4 DHCP Properties

The following sections describe how to configure properties that apply to IPv4 DHCP objects only. You can configure and define the following DHCP properties:

- General properties, as described in [Configuring General IPv4 DHCP Properties](#).
- Ping settings, as described in [Configuring Ping Settings](#).
- DHCP lease management, as described in [Configuring DHCP Lease Management](#).
- BOOTP and PXE properties, as described in [Configuring IPv4 BOOTP and PXE Properties](#).
- Custom DHCP options, as described in [About IPv4 DHCP Options](#).
- DDNS settings, as described in Chapter 21, [Configuring DDNS Updates](#).
- Ignore DHCP client identifiers, as described in [Ignoring DHCP Client Identifiers](#).
- Thresholds for DHCP ranges, as described in [Configuring Thresholds for DHCP Ranges](#).

For information on configuring properties that apply to IPv4 and IPv6 DHCP objects, see [Configuring DHCP IPv4 and IPv6 Common Properties](#).

**Note**: Limited-access admin groups can access certain DHCP resources only if their administrative permissions are defined. For information on setting permissions for admin groups, see [Administrative Permissions for DHCP Resources](#).

### Configuring Thresholds for DHCP Ranges

Grid Manager can provide a view of the current overall DHCP range usage for the DHCP ranges defined on each Grid member. The view is in the form of a percent: address leases in use/total addresses for each network. Such information can indicate if there is a sufficient number of available addresses at each of these levels. It can also provide information about the distribution of address resources, indicating if there are too many unused addresses in one location while all the addresses in another are in use.

In addition to viewing the percent of addresses in use, you can also apply high and low thresholds for each DHCP range. These watermarks represent thresholds above or below which DHCP range usage is unexpected and might warrant your attention. For example, usage falling below a low threshold might indicate network issues preventing the renewal of leases. When usage for a DHCP range crosses a threshold, the appliance makes a syslog entry and — if configured to do so — sends the administrator alerts as SNMP traps and email notifications. Figure 26.2 illustrates the relationship of allocated and available addresses to high and low watermarks in a DHCP range.

*Figure 26.2 Overall DHCP Address Usage for a DHCP Range*
You can define watermarks at the Grid, member, network, and DHCP range levels, but the appliance applies them solely to DHCP ranges. Because the appliance applies settings hierarchically in a parent-child structure, by defining watermarks once at a higher level, DHCP ranges can then inherit these settings without your needing to redefine them for each range. For example, if you set high and low watermarks for a Grid, then each Grid member, each network, and each DHCP range inherits these settings. However, if you override these settings at the member level, then the network and DHCP ranges for that member inherit its settings. If you override the Grid member settings at the network level, then that network and any DHCP ranges within that network inherit the network-level settings. Finally, you can set high and low watermarks for an individual DHCP range, which override anything set at a higher level.

Figure 26.3 shows different high and low watermark settings at different levels. Although you can set thresholds at four levels (Grid, Grid member, network, and DHCP range), the NIOS appliance applies them to DHCP ranges.

You can set DHCP range usage thresholds (watermarks) 20% for Grids, Grid members, networks, and DHCP ranges.

The thresholds that you set at more narrowly defined levels override thresholds set at the more generic levels that contain them. For example, if address usage exceeds the 70% high watermark or dips below the 30% low watermark for the DHCP range shown here, the NIOS appliance generates email and SNMP alerts, even though address usage is within acceptable ranges at all higher levels.

There is a parent-child relationship among different levels. If you do not set a watermark at a more specific level, it inherits the setting from a higher level that contains it.

Note: You can set watermarks at different levels, but the appliance applies only watermarks that are set or inherited at the DHCP range.
Address usage in a DHCP range can trigger an event and an email notification when it crosses a watermark. You must enable DHCP threshold and email warnings to receive events and notifications. The following are actions that do and do not trigger an address usage event and notification:

- **Address usage triggers an event and the appliance sends a notification when the percentage of the allocated addresses in the DHCP range:**
  - Exceeds the high watermark
  - Drops below or equals to the high watermark after exceeding it
  - Drops below the low watermark
  - Exceeds the low watermark after dropping below it

- **Address usage does not trigger an event when the percentage of the allocated addresses in the DHCP range:**
  - Never exceeds the low watermark
  - Initially exceeds the low watermark
  - Reaches a watermark but does not cross it

**Note:** You can effectively disable address usage events for a DHCP range by setting its high watermark at 100% and the low watermark at 0% (default setting for the low watermark). Because address usage cannot cross these watermarks, no events can occur.

You can configure the threshold settings at the Grid level and override them at the member, network, and DHCP range levels. To override an inherited DHCP property, click **Override** next to the property to enable the configuration. For information, see [Overriding DHCP Properties](#).

To configure thresholds:

1. **Grid:** From the **Data Management** tab, select the **DHCP** tab, and then click **Grid DHCP Properties** from the Toolbar.
   - **Member:** From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **Members** -> **member** check box, and then click the **Edit** icon.
   - **Network:** From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** check box, and then click the **Edit** icon.
   - **Network Container:** From the **Data Management** tab, select the **IPAM** tab -> **network_container** check box, and then click the **Edit** icon.
   - **DHCP Range:** From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** -> **addr_range** check box, and then click the **Edit** icon.

2. In the editor, select the **IPv4 DHCP Thresholds** tab and complete the following:
   - **DHCP Thresholds:** Specify the following:
     - **Enable DHCP Thresholds:** Select **Enable DHCP Thresholds** to enable the DHCP threshold feature.
     - **High:** Enter a number between 0 and 100. Enter Trigger and Reset values. If the percentage of allocated addresses in a DHCP range exceeds the Trigger value, the appliance makes a syslog entry and—if configured to do so—sends an SNMP trap and an email notification to a designated destination. When the percentage first reaches the Reset value after it hit the Trigger value, the appliance sends an SNMP trap and an email notification to a designated destination. The default Trigger value is 95, and the default Reset value is 85.
     - **Low:** Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range drops below the Trigger value, the appliance makes a syslog entry and—if configured to do so—sends an SNMP trap and an email notification to a designated destination. When the percentage first reaches the Reset value after it hit the Trigger value, the appliance sends an SNMP trap. The default Trigger value is 0 and the default Reset value is 10.
   - **Enable SNMP Warnings:** Select this for the appliance to send an SNMP trap to the trap receiver that you define for the Grid when the address usage in a DHCP range crosses a high or low mark threshold.
   - **Enable Email Warnings:** Select this for the appliance to send an email notification to an administrator if the address usage in a DHCP range crosses a high or low mark threshold.
   - **Email Addresses:** Click **Override** to override the Grid administrator email address configured in the **Data Management** tab -> **Grid** tab. This address is not hierarchically inherited from the Grid DHCP configuration. Click the **Add** icon, and then enter an email address to which you want the appliance to send email notifications when the DHCP range for the network crosses a threshold. You can create a list of email addresses.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

### Configuring DHCPv6 Properties

The following sections describe how to configure properties and options that apply to DHCPv6 objects only. You can configure and define the following DHCP properties:

- General properties, as described in the next section, **Defining General IPv6 Properties**.
- DHCP options, as described in **About DHCPv6 Options**.

### Defining General IPv6 Properties

You can configure general DHCPv6 properties at the Grid level and override them at the member and lower levels.

1. **Grid:** From the **Data Management** tab, select the **DHCP** tab, and then click **Grid DHCP Properties** from the Toolbar.
   - **Member:** From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **Members** -> **member** check box, and then click the **Edit** icon.
About DHCPv6 Options

DHCPv6 options provide configuration and service information to IPv6 clients. Just like IPv4 options, IPv6 options appear as variable length fields at the end of the DHCPv6 messages.

Just as in IPv4, the NIOS appliance supports the following options in the DHCPv6 options space:

- **Predefined options**: These are the option codes defined in RFC 3315. You cannot redefine these options or delete them from the DHCP option space. Option codes 1-48 are reserved and cannot be used to define custom options.
- **Custom options**: These are option codes 49 to 254. They are not defined by IETF standards and are available for private use. You can use these option codes to provide configuration or service information that none of the predefined options provide.

You can also create option spaces to define new groups of options. For example, you can create additional option spaces to define vendor specific options, which are encapsulated in DHCPv6 option 17. When an IPv6 client requests vendor specific options, it makes a request using the vendor specific options (option 17). The DHCP server then responds with the list of replies for the various options encapsulated into option 17. Note that custom options defined in the DHCP option space are included in the options section of the DHCP messages that DHCP servers and clients exchange.

You can apply options globally at the Grid level, or more specifically at the member, network, range, host and roaming host levels.

Configuring DHCPv6 Options

To use DHCPv6 options, you can do the following:

- Configure one or more option spaces, as described in the next section Defining IPv6 Option Spaces.
- Define custom options in the predefined DHCPv6 option space or add options to an option space that you configured. For more information, see Configuring Custom DHCP Options.
- Specify values for the options and apply them to the Grid, or to a member, network, fixed address, host, or roaming host. For more information, see Applying DHCPv6 Options.

Defining IPv6 Option Spaces

DHCP members support the DHCPv6 option space by default. You can create additional option spaces to provide additional configuration or service information.

To add a custom option space:

1. From the Data Management tab, select the DHCP tab -> Option Spaces tab.
2. Click the Add icon -> IPv6 Option Space.
3. In the IPv6 Option Space wizard, do the following:
   - **Name**: Enter the name of the option space.
   - **Enterprise Number**: Enter the vendor's Enterprise Number that is registered with IANA.
   - **Comment**: Enter useful information about the option space.
   - **Options**: Click the Add icon to add options. For additional information, see the next section, Configuring Custom DHCP Options.
4. Save the configuration and click Restart if it appears at the top of the screen.

After you create an option space and add options to it, you can apply the options as described in Applying DHCP Options.

Configuring Custom IPv6 DHCP Options

You can define custom options in the DHCP option space or in an option space that you configured, as follows:

1. From the Data Management tab, select the DHCP tab -> Option Spaces tab.
2. Select either the DHCPv6 option space or an IPv6 option space that you configured, and then click the Edit icon.

3. In the Option Space editor, click the Add icon to add a custom option. In the new row, complete the following:
   - **Name**: Enter the name of the custom DHCP option.
   - **Code**: Enter a number from 1 to 65535 to add a custom option in the DHCP option space or in an IPv6 option space that you have configured.
   - **Type**: Select the option type (such as ipv6-address, text, boolean, and string as described in Table 26.2).

   Click the Add icon to add more options.

4. Save the configuration.

### Applying DHCPv6 Options

You can apply some options at the Grid or member level, and some options to specific networks, shared networks, fixed addresses and roaming hosts. When you apply an option, you select the object to which the option is applied, such as the Grid, member, or network, and then specify a value for the option.

Use the following guidelines when specifying option values:

- Enter `false` or `true` for a Boolean Flag type value.
- Enter an ASCII text string, or enter a series of octets specified in hex, separated by colons.
- Separate multiple values by commas. For example, to enter multiple IP addresses for netbios-name-servers, enter a comma between each IP address.

DHCPv6 options support the same data types as DHCP IPv4 options. For more information about the data types, see [DHCP Option Data Types](#).

To apply DHCP options:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then select Grid DHCP Properties from the Toolbar.  
   - **Member**: From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.
   - **Network**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.
   - **Network Container**: From the Data Management tab, select the IPAM tab -> network_container check box, and then click the Edit icon.
   - **Fixed Address**: From the Data Management tab, select the DHCP tab -> Networks tab -> Network -> fixed_address check box, and then click the Edit icon.
   - **Host Address**: From the Data Management tab, select the DHCP tab -> Networks tab -> Network -> host_record check box, and then click the Edit icon. Select the host IP address, and then click the Edit icon.
   - **Roaming Host**: From the Data Management tab, select the DHCP tab -> Networks tab -> Roaming Hosts -> roaming_host check box, and then click the Edit icon.

2. In the DHCP Properties editor, select the IPv6 DHCP Options and complete the following:
   - **Custom IPv6 DHCP Options**: In the first field, select one of the following from the drop-down list:
     - **DHCPv6**: Select this to apply DHCPv6 options.
     - **DHCP**: Select this to apply DHCP options (dhcp-renewal-time or dhcp-rebinding-time).

   In the second field, click the Choose option arrow and select an option from the list. In the third field, enter a value for the selected option.

   Note that certain options have predefined data types and their values must be entered in a specific format. For information about the data types, see [DHCP Option Data Types](#).

   Click + to add another option, or click - to delete a previously specified option. When overriding an option, enter the new value for the selected option.

   Note that if you created an option space, this section displays a list of option spaces in the first drop-down menu, so you can select the option space of the option you want to define.

3. Save the configuration and click Restart if it appears at the top of the screen.

### Configuring DHCP IPv4 and IPv6 Common Properties

This section describes DHCP properties that apply to both IPv4 and IPv6. It includes the following sections:

- **Configuring UTF-8 Encoding for Hostnames**
- **Associating Networks with Zones**
- **Keeping Leases in Deleted IPv4 and IPv6 Networks and Ranges**
- **Configuring Fixed Address Leases For Display**
- **Scavenging Leases**
- **DHCPv6 Lease Affinity**

### Configuring UTF-8 Encoding for Hostnames

When you configure the appliance as a DHCP server, the appliance supports UTF-8 encoding of hostnames that are encoded with Microsoft Windows code pages. You can configure the DHCP services on the appliance to convert these client hostnames to UTF-8 characters. The appliance stores the UTF-8 encoded hostnames in the database. If you also configure the DHCP services on the appliance to perform DDNS
updates, the appliance sends the UTF-8 encoded host names in the DDNS updates. You can configure the UTF-8 encoding of host names at the Grid DHCP service and member DHCP service levels. For information on UTF-8 encoding, see Printing from Grid Manager.

The appliance displays the host names in their original characters in the following:

- DHCP lease history
- DHCP lease details
- IP address management
- Syslog
- Audit log

To configure UTF-8 encoding for hostnames:

1. **Grid:** From the Data Management tab, select the DHCP tab, and then select Grid DHCP Properties from the Toolbar.
2. In the DHCP Properties editor, select the General Basic tab and complete the following:
   - IPv4 Properties
     - **Microsoft Clients Code Page:** From the drop-down list, select the code page with which the host names are encoded when the appliance converts the Microsoft code page encoded host names to UTF-8 characters.
   - IPv6 Properties
     - **Microsoft Clients Code Page:** From the drop-down list, select the code page with which the host names are encoded when the appliance converts the Microsoft code page encoded host names to UTF-8 characters.
3. Save the configuration and click Restart if it appears at the top of the screen.

### Associating Networks with Zones

You can associate IPv4 and IPv6 networks with DNS zones to limit the zones that admins can use when they create DNS records for IP addresses in the networks. When a network is associated with one or more zones and an admin creates a DNS record for one of its IP addresses, Grid Manager allows the admin to create the DNS record in the associated zones only. For example, if you associate the 10.1.0.0/16 network with the corp200.com zone, admins are allowed to create DNS records in the corp200.com zone only for IP addresses in the 10.1.0.0/16 network; or if you associate the 2001:db8:1::/48 network with the corp200.com zone, admins are allowed to create DNS records in the corp200.com zone only for IP addresses in the 2001:db8:1::/48 network.

This feature applies to A, AAAA and host records only. It does not apply to records in a shared record group. If you are creating a host record with multiple IP addresses in different networks, the networks must be associated with the zone of the host record.

If a network is not associated with a zone, admins can create DNS records for its IP addresses only in zones with no network associations as well. You can associate a network with any authoritative zone whose primary server is a Grid member or a Microsoft server, or is unassigned. You cannot associate networks with zones that have external primary servers.

You can associate a network with multiple zones, and associate a zone with more than one network. You can associate IPv4 and IPv6 network containers and networks with zones. When you associate a network container with zones, its networks inherit the zone associations. You can override the zone associations at the network level.

Associated DNS records must have IP addresses in the networks. When a network is associated with one or more zones and an admin creates a DNS record for one of its IP addresses, Grid Manager allows the admin to create the DNS record in the associated zones only. For example, if you associate the 10.1.0.0/16 network with the corp200.com zone, admins are allowed to create DNS records in the corp200.com zone only for IP addresses in the 10.1.0.0/16 network; or if you associate the 2001:db8:1::/48 network with the corp200.com zone, admins are allowed to create DNS records in the corp200.com zone only for IP addresses in the 2001:db8:1::/48 network.

This feature applies to A, AAAA and host records only. It does not apply to records in a shared record group. If you are creating a host record with multiple IP addresses in different networks, the networks must be associated with the zone of the host record.

If a network is not associated with a zone, admins can create DNS records for its IP addresses only in zones with no network associations as well. You can associate a network with any authoritative zone whose primary server is a Grid member or a Microsoft server, or is unassigned. You cannot associate networks with zones that have external primary servers.

You can associate a network with multiple zones, and associate a zone with more than one network. You can associate IPv4 and IPv6 network containers and networks with zones. When you associate a network container with zones, its networks inherit the zone associations. You can override the zone associations at the network level.

If you split a network, the resulting subnets inherit the zone associations. If you join networks, the resulting network retains the zone associations of the network that you selected when you performed the join operation. You can override the inherited zone associations of individual networks.

Subzones do not inherit the network associations of their parent zones. When you import data into a zone that is associated with a list of networks, the imported A, AAAA and host records must have IP addresses in the associated networks. Grid Manager does not allow you to import A, AAAA and host records with IP addresses in unassociated networks.

When you associate a network with a zone, the DNS records created before the association are not affected. But if you edit an A, AAAA or host record after the association, Grid Manager does not allow you to save the record if its IP address is not in an associated network.

To associate an IPv4 or IPv6 network with a zone:

1. From the Data Management tab, select the DHCP tab -> Networks -> Networks -> network check box, and then click the Edit icon.
2. In the DHCP Network editor, click Toggle Advanced Mode if the editor is in basic mode.
3. When the additional tabs appear, click the Advanced subtab of the General tab.
4. Click the Add icon and select the zone you want to associate with the network.
5. Optionally, select a default zone. When you create or edit an A, AAAA or host record from a network in the IPAM tab, Grid Manager automatically selects the default zone that is assigned to the network.

5. Save the configuration or click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

### Viewing the Networks Associated with a Zone

You can view the IPv4 or IPv6 networks associated with a zone from the zone editor. The tab to display network associations in zone editors is visible only if the primary server is a Grid member, a Microsoft server, or unassigned.

To view the network associations of a zone:

1. From the Data Management tab, select the DNS tab -> Zones -> zone check box, and then click the Edit icon.
2. In the Authoritative Zone editor, click Toggle Advanced Mode if the editor is in basic mode.
3. When the additional tabs appear, click the Advanced subtab of the General tab.

The Network Associations table lists the networks and their corresponding comments. You cannot change the network associations in this editor.
Navigate to the DHCP Network editor of the network, to change the zone associations.

**Keeping Leases in Deleted IPv4 and IPv6 Networks and Ranges**

You can configure the DHCP server to store leases in a deleted DHCP range for up to one week after the leases expire. When you add a new DHCP range that includes the IP addresses of these leases or assign the DHCP range to another member within the Grid, the appliance automatically restores the active leases. You can configure this feature for the Grid, and override the configuration for members, networks, and DHCP ranges.

To keep active leases in a deleted DHCP range:

1. **Grid:** From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
   - **Member:** From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.
   - **Network:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.
   - **Network Container:** From the Data Management tab, select the IPAM tab -> network_container check box, and then click the Edit icon.
   - **Range:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> range check box, and then click the Edit icon.

2. In the DHCP Properties editor of the Grid or member, click **Toggle Advanced Mode** if the editor is in basic mode, and then click the General tab -> Advanced tab. In the Network editor or Range editor, click **Toggle Advanced Mode** if the editor is in basic mode, and then click IPv4 DHCP Options -> Advanced or IPv6 DHCP Options -> Advanced. Complete the following:
   - **IPv4 Properties**
     - **Lease Deletion:** When you select *Keep leases from deleted range until one week after expiration* and delete a DHCP range with active leases, the appliance stores these leases for up to one week after they expire.
   - **IPv6 Properties**
     - **Lease Deletion:** When you select *Keep leases from deleted range until one week after expiration* and delete a DHCP range with active leases, the appliance stores these leases for up to one week after they expire.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

**Configuring Fixed Address Leases For Display**

You can configure the DHCP server to capture the hostname and lease time of a fixed address when you assign an IPv4 or IPv6 fixed address to a client. The appliance displays the hostname, and the start and end time of each fixed address lease in the **Current Leases** panel in Grid Manager.

You can set this at the Grid level only for IPv4 and IPv6 leases.

1. From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
2. In the Grid DHCP Properties editor, click **Toggle Advanced Mode** if the editor is in basic mode. When the additional tabs appear, click the General tab -> Advanced tab and complete the following:
   - **IPv4 Properties**
     - **Fixed Address Lease:** Select Capture hostname and lease time when assigning Fixed Addresses. The appliance displays the host name, and the start and end time of each fixed address lease in the **Current Leases** panel. If there are multiple records (A, host, and lease) for the IP address, it also displays the information for the records. This option is available in the Grid Properties editor only.
   - **IPv6 Properties**
     - **Fixed Address Lease:** Select Capture hostname and lease time when assigning Fixed Addresses. The appliance displays the host name, and the start and end time of each fixed address lease in the **Current Leases** panel. If there are multiple records (AAAA, host, and lease) for the IP address, it also displays the information for the records. This option is available in the Grid Properties editor only.

3. Save the configuration.

**Scavenging Leases**

The accumulation of free and backup DHCPv4 leases; and free, expired, and released DHCPv6 leases results in unnecessary growth of database objects. The DHCP lease scavenging feature enables member DHCP servers to automatically delete free and backup IPv4 leases; and free, expired, and released IPv6 leases that remain in the database beyond the specified period of time, thus reducing the number of database objects.

When you enable this feature for DHCPv4 leases, the appliance permanently deletes the free and backup IPv4 leases, and you can no longer view or retrieve the lease information. This option can be enabled globally at the Grid level, and more specifically for a member, shared network, network, network container, DHCP range, network template, DHCP range template.

When you enable this feature for DHCPv6 leases, the appliance permanently deletes the free, expired, and released IPv6 leases, and you can no longer view or retrieve the lease information. This option can be enabled at the Grid level, and overridden at the member level.

The period of time that you specify is the duration after the expiration date of a lease, not its release date. For example, you specify a time period of 5 days when you enable this feature. If the lease time of an IP address is 10 days, but the lease is released after five days, the appliance still deletes the lease from the database after 15 days because the IP address has been leased.

---

**Note:** If you plan to enable this feature after upgrading from a previous NIOS version, Infoblox recommends that you enable it during off-peak hours, as it may impact DHCP services.
To enable scavenging of IPv4 and IPv6 leases:

1. **Grid**: From the **Data Management** tab, select the **DHCP** tab, and then click **Grid DHCP Properties** from the **Toolbar**.
   - **Member**: From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **Members** -> member check box, and then click the **Edit** icon.
   - **Network**: From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** check box, and then click the **Edit** icon. This is applicable for IPv4 lease scavenging only.
   - **Network Container**: From the **Data Management** tab, select the **IPAM** tab -> **network_container** check box, and then click the **Edit** icon. This is applicable for IPv4 lease scavenging only.
   - **DHCP Range**: From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** -> **addr_range** check box, and then click the **Edit** icon. This is applicable for IPv4 lease scavenging only.

2. In the editor, click **Toggle Advanced Mode** if the editor is in basic mode, and then click the **General** tab -> **Advanced** tab.

   In the Network editor for IPv4 lease scavenging, click **Toggle Advanced Mode** if the editor is in basic mode, and then click **IPv4 DHCP Options** -> **Advanced**.

   Complete the following:

   - **IPv4 Properties**
     - **Lease Scavenging**: This is disabled by default. Select the **Scavenge free and backup leases after** check box and specify the number of days or weeks that free and backup IPv4 leases remain in the database before they are automatically deleted. This can be set for the Grid, member, network, and network container.
   - **IPv6 Properties**
     - **Lease Scavenging**: This is disabled by default. Select the **Scavenge free, expired and released leases after** check box and specify the number of days or weeks that free, expired, and released IPv6 leases remain in the database before they are automatically deleted. The minimum is 6 hours and the maximum is 180 days. The default is one week. This can be set at the Grid and member level.

3. Save the configuration.

### DHCPv6 Lease Affinity

DHCPv6 ranges are usually large and the DHCPv6 server randomly selects a new lease each time a client requests for a lease. The client can use the lease until it expires. After its expiration, the lease stays in the database with an expired state. These expired leases eventually lead to the increase in the number of database objects, because the probability of expired IPv6 leases getting reused is low.

Infoblox provides a DHCPv6 lease affinity feature that allows you to reuse expired IPv6 leases for DHCP clients. When you enable this feature, the DHCPv6 server automatically renews the expired leases. A DHCP client can retrieve the same lease from the DHCPv6 server after it expires and retains the same IP address. This feature helps reduce the amount of IPv6 leases in the database as the DHCP server issues the same lease multiple times for the same client.

The appliance ignores expired leases that are older than the specified period. Such leases are scavenged. Note that the grace period you define for lease scavenging is applicable for DHCPv6 lease affinity also. The minimum time period is six hours, maximum is 180 days and the default is set to seven days. For more information about scavenging leases, see **Scavenging Leases**.

**Note**: The DHCPv6 server offers the same lease for a DHCP client, identified by DUID, after the lease expires and before the end of the grace period. The appliance removes the expired leases that are older than the grace period from the database.

DHCPv6 lease affinity and DHCPv6 lease scavenging are complementary features. For example, consider a scenario in which a visiting user gets an IPv6 lease that is retained for days, weeks, or months depending on the needs and then the user leaves. If the user returns and the lease is still within the grace period, the user gets the same IPv6 lease. This is lease affinity. When the user leaves, the IPv6 lease becomes inactive. This lease is scavenged after the grace period.

Note the following about DHCPv6 lease affinity:

- It does not consider expired leases that are older than the grace period.
- It ignores expired leases that do not match known ranges.
- If no existing lease is found, then the DHCPv6 server finds a suitable expired lease that is not older than the grace period, which matches the client DUID and range configuration.
- The impact of the feature on the performance depends on the amount of expired DHCPv6 leases.
- When you activate the feature at the Grid level, it affects all underlying layers of inheritance.
- You cannot enable DHCPv6 lease affinity at the Grid and member levels during a scheduled full upgrade.
- DHCPv6 lease affinity remembers only permanent addresses and does not remember temporary addresses and prefix delegations.
- If the DHCPv6 range is out of available addresses when you enable DHCPv6 lease affinity, then the DHCP server tries to reuse the best abandoned lease, which indicates the lease that was abandoned longest time ago. If there are no such leases in the pool, the DHCP server reuses the best expired lease, which indicates the lease that expired longest time ago. This means that the expired lease becomes active and it is associated with the new client while the DHCP server removes any previous associations of the corresponding lease. Note that this happens only when the DHCPv6 range does not have any available addresses and there are no suitable abandoned leases.

To enable DHCPv6 lease affinity:

1. **Grid**: From the **Data Management** tab, select the **DHCP** tab, and then click **Grid DHCP Properties** from the **Toolbar**.
   - **Member**: From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **Members** -> member check box, and then click the **Edit** icon.
2. In the editor, click **Toggle Advanced Mode** if the editor is in basic mode, and then click the **General** tab -> **Advanced** tab.

Complete the following:

- **IPv6 Properties**
  - **Lease Scavenging**
    - **Remember client association for expired members**: This is disabled by default. Select the check box to remember and reuse expired IPv6 leases that are associated with DHCP clients. You can select this check box only when you select the **Scavenge free, expired and released leases after** check box. This can be set at the Grid and member levels.

**Note**: The appliance stores the leases, which are either deleted or removed, in the recycle bin. These leases then become free and are automatically dissociated from their clients. For example, if you delete a range accidentally and restore it again, the IPv6 leases associated with the respective range are no longer associated with the same set of clients.

3. Save the configuration.

### Configuring DHCP Logging

If you have a syslog server operating on your network, you can specify in which facility you want the server to display the DHCP logging messages. You can also select the Grid member on which you want to store the DHCP lease history log, as described in the next section **Configuring the Lease Logging Management**. You can configure DHCP and lease logging only on the Grid and member levels.

To specify DHCP logging for the Grid or member:

1. **Grid**: From the **Data Management** tab, select the **DHCP** tab, and then click **Grid DHCP Properties** from the Toolbar.

   **Member**: From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **Members** -> member check box, and then click the **Edit** icon.

2. In the **DHCP Properties** editor, select the **Logging Basic** tab and complete the following:
   - **Syslog Facility**: From the drop-down list, select the facility that is used to tag syslog messages from the DHCP server. This facility can be used to filter messages on a central syslog server.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

### Configuring the Lease Logging Member

Logging DHCP lease events makes significant CPU demands, especially when there is heavy DHCP activity. Therefore, Infoblox strongly recommends that you designate a Grid member other than the master as a logging member whenever possible. Another way to manage the increased load that logging introduces is to log selectively per Grid member. For example, you might want to log DHCP leases for members serving critical parts of your network and not keep historical logs for members serving other parts.
You can enable DHCP lease logging at the Grid level, and then disable it for selected members. In this Grid, four members serve DHCP lease events to the master, which forwards them to a designated logging member. Two Grid members do not log DHCP lease events.

To specify lease logging for a member:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
   **Member**: From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.

2. In the Logging tab, complete the following:
   - **Lease Logging**: Select Enable Lease History (for Grid) or Log Lease Events from DHCP Server (for member) to enable DHCP lease logging. To disable DHCP lease logging, clear the check box. You can set member overrides if you want to enable or disable lease logging per member.
   - **Send leases to**: For Grid only. Click Select. In the Select Member dialog box, select the Grid member on which you want to store the DHCP lease history log. Infoblox recommends that you dedicate a member other than the Grid Master as a logging member. If possible, use this member solely for storing the DHCP lease history log. If you do not select a member, no logging can occur. You can click Clear to remove the selected Grid member and select a new one.

3. Save the configuration and click Restart if it appears at the top of the screen.

**Note**: You cannot configure vNIOS Grid members on Riverbed as DHCP lease history logging members.

4. For information about viewing current leases, see Viewing Current Leases.

**About IF-MAP**

You can configure Infoblox DHCP servers to publish DHCP data to an IF-MAP server. The IF-MAP server takes real-time information from different sources and stores it in a shared database from which clients can retrieve information about network devices, their status and activities. For details about the IF-MAP protocol, refer to http://www.trustedcomputinggroup.org. For information about the Infoblox IF-MAP server, refer to
the Infoblox Administrator Guide for Infoblox Orchestration Server.

Each Infoblox DHCP server in a Grid can function as an IF-MAP client, with the ability to publish lease information to an IF-MAP server. For information about how to configure an IF-MAP client, see Configuring Members as IF-MAP Clients. You can configure the client to publish ip-mac and ip-duid (for DHCPv6 leases) metadata at the Grid and member levels. You can also configure the client to publish metadata for specific leases by overriding the Grid or member publishing settings at the network (IPv4 and IPv6) or range (IPv4 only) level. The DHCP server sends updates to the IF-MAP server using the XML format and SOAP/HTTPS bindings specified in IF-MAP v1.1r5 and v2.0r26. The DHCP server supports the IF-MAP 2.0 protocol by default. You can also enable the support for IF-MAP 1.1, as described in Configuring a Grid to Support IF-MAP.

When the DHCP server grants an IPv4 lease and sends the DHCPACK packet to the DHCP client, it updates the link in the IF-MAP server between the leased IP address and client MAC address with ip-mac metadata with the following attributes: start-time, end-time, and dhcp-server. The dhcp-server attribute contains the DHCP server hostname. The ip-mac metadata is attached to a link with:

- An ip-address identifier with the type attribute set to IPv4, a value attribute that contains the leased IP address, and the administrative-domain attribute set to the network view to which the IP address belongs.
- A mac-address identifier with a value attribute that contains the client MAC address. It does not have the administrative-domain attribute.

When the DHCP server grants an IPv6 lease and sends the Reply message to the DHCP client, it updates the link in the IF-MAP server between the leased IP address and client DHCP Unique Identifier (DUID) with ip-duid metadata that contains the following attributes: start-time, end-time, and dhcp-server. The dhcp-server attribute contains the DHCP server hostname. The ip-duid metadata is attached to a link with:

- An ip-address identifier with the type attribute set to IPv6, a value attribute that contains the leased IP address, and the administrative-domain attribute set to the network view to which the IP address belongs.
- A duid identifier with a value attribute that contains the client DUID. It does not have the administrative-domain attribute.

The Infoblox DHCP server also publishes data when an IPv4 or IPv6 lease changes. When a lease is released or when an active lease expires, the DHCP server sends a "publish delete" request to the IF-MAP server.

You can define how the IF-MAP server handles the existing ip-mac and ip-duid information before the DHCP client sends the next update. For example, you can specify the IF-MAP server to always delete existing ip-mac and ip-duid information before the next update. For information, see Deleting Existing Data Before Publishing.

Following are the tasks to enable DHCP servers in a Grid to function as IF-MAP clients:

1. Enable IF-MAP in the Grid and specify the URL and port of the IF-MAP server, as described in Configuring a Grid to Support IF-MAP.
2. Optionally, enable the validation of the IF-MAP server certificate and import the CA certificate, as described in Validating the IF-MAP Server Certificate.
3. Enable IF-MAP on each Grid member and specify an authentication method the member uses to connect to the IF-MAP server, as described in Configuring Members as IF-MAP Clients.
4. Optionally, override publishing settings at the member, network, or range level, as described in Overriding IF-MAP Publishing Settings.

You can also delete DHCP data published by a specific member, or define how the IF-MAP server deletes existing DHCP data before a client publishes an update. For information, see Deleting Data from the IF-MAP Server.

Configuring a Grid to Support IF-MAP

1. From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
2. In the Grid DHCP Properties editor, click Toggle Advanced Mode.
3. Click the IF-MAP tab, and then complete the following:
   - Enable IF-MAP: Select this check box to enable the IF-MAP service for the Grid. Note that you must enable the IF-MAP service in order to enable or disable publishing at the Grid, member, network, or range level.
   - IF-MAP Server URL: Enter the URL of the IF-MAP server to which the Grid members publish DHCP data. The URL must begin with https://. For example, https://<server_ip_addr>/ifmap.
   - IF-MAP Server Port: The default HTTP port is 80 and the default HTTPS port is 443. Optionally, you can specify a different port on the IF-MAP server.
   - Enable IF-MAP publishing: Select this check box to enable IF-MAP publishing for the Grid. When you select this, IF-MAP publishing is enabled for all members, networks (IPv4 and IPv6), and DHCP ranges (IPv4 only). You can override the Grid property at a specific level to control the ip-mac and ip-duid metadata you want the client to publish for specific leases. For information, see Overriding IF-MAP Publishing Settings.
   - IF-MAP Protocol Version: Select the IF-MAP protocol version you want the IF-MAP client to use to connect to the IF-MAP server. The default is IF-MAP 2.0.
4. Save the configuration and click Restart if it appears at the top of the screen.
5. You can also configure how the IF-MAP server deletes existing metadata before the IF-MAP client publishes another update. For information, see Deleting Data from the IF-MAP Server.

Validating the IF-MAP Server Certificate

You can configure the IF-MAP client to validate the IF-MAP server certificate before the client establishes a connection or performs IF-MAP transactions. To validate an IF-MAP server certificate, you must first import the certificate of the CA that signs the IF-MAP server certificate.

To configure the IF-MAP client to validate the IF-MAP server certificate:

1. From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
2. In the Grid DHCP Properties editor, click Toggle Advanced Mode.
3. Click the **IF-MAP** tab and complete the following:
   - **Enable IF-MAP**: Select this check box to enable the IF-MAP service for the Grid.
   - **Enable IF-MAP server certificate validation**: Select this check box to enable the validation of the IF-MAP server certificate, and then click **Import** to import the CA certificate. In the **Upload** dialog box, click **Select** to navigate to the certificate, and then click **Upload**. You can also copy and paste the CA certificate here.
4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Configuring Members as IF-MAP Clients

To configure a member to be an IF-MAP client, you must first enable IF-MAP on the member and then configure a client authentication method. The IF-MAP client can authenticate itself to the IF-MAP server through user name and password credentials or digital certificate. Note that each member must have unique credentials or certificates. You cannot use the same credentials or certificates on multiple members. The appliance supports only one CA-signed certificate on each member. If you want to use a roll-over certificate, you must replace the existing certificate and restart services on the member.

To enable an appliance to function as an IF-MAP client:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box, and then click the **Edit** icon.
2. In the **Member DHCP Properties** dialog box, click **Toggle Advanced Mode**.
3. Click the **IF-MAP** tab and complete the following:
   - **Enable IF-MAP**: Select this check box to enable the IF-MAP service on the member. Note that you must enable the IF-MAP service in order to enable or disable publishing at the network and range levels.
   - **Authentication**: Select one of the following authentication methods:
     - **Certificate**: Select this to use the IF-MAP client certificate for client authentication. You must already have a certificate configured for the member before you can select and save this configuration. For information about creating a client certificate, see **Creating IF-MAP Client Certificates**.
     - **Basic**: Select this to use username and password credentials for IF-MAP client authentication.
   
   Complete the following:
   - **Username**: Enter the username the member uses to connect to the IF-MAP server. This username must have been configured as a valid username on the IF-MAP server. Each member must have its own username.
   - **Password**: Enter the password the member uses to connect to the IF-MAP server.
   - **ConfirmPassword**: Enter the password again.

   **Note**: When you upgrade to a new NIOS release, the basic authentication credentials are retained if IF-MAP was enabled and basic authentication was used before the upgrade.

   - **Enable IF-MAP publishing**: Click **Override** to override the Grid setting. Select this check box to enable IF-MAP publishing for all the networks that are served by this member. Ensure that you enable IF-MAP at either the Grid or member level in order to enable IF-MAP publishing for all networks.
4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Creating IF-MAP Client Certificates

Before you can select "Certificate" as the client authentication method, you must first create a certificate for the specified member. You can do one of the following to generate an IF-MAP client certificate:

- Generate a self-signed certificate and save it. For information, see **Generating Self-Signed Certificates**.
- Request a CA (Certificate Authority) signed certificate. When you receive the certificate from the CA, upload it to the member that you configure as an IF-MAP client. For information, see **Generating Certificate Signing Requests**.

### Generating Self-Signed Certificates

You can replace the default certificate with a self-signed certificate that you generate. When you generate a self-signed certificate, you can specify the correct hostname and change the public/private key size, enter valid dates and specify additional information specific to the member. If you have multiple members, you can generate a certificate for each appliance with the appropriate hostname.

To generate a self-signed certificate:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box, and then click **IF-MAP Client Certificate** -> **Generate Self-signed Certificate** from the Toolbar.
2. In the **Generate Self-signed Certificate** dialog box, complete the following:
   - **Secure Hash Algorithm and Key Size**: You can select SHA-1 and a RSA key size of 1024 or 2048. SHA-256 (SHA-2) can be selected together with a RSA key size of 2048 or 4096. The default value is SHA-256 2048.
   - **Days Valid**: Specify the validity period of the certificate.
   - **Common Name**: Specify the domain name of the member. You can enter the FQDN (fully qualified domain name) of the appliance.
   - **Organization**: Enter the name of your company.

Copyright ©2019, Infoblox, Inc. All right reserved.
• **Organizational Unit**: Enter the name of your department.
• **Locality**: Enter a location, such as the city or town of your company.
• **State or Province**: Enter the state or province.
• **Country Code**: Enter the two-letter code that identifies the country, such as US.
• **Admin E-mail Address**: Enter the email address of the appliance administrator.
• **Comment**: Enter information about the certificate.

3. Click **OK**.

4. If the appliance already has an existing client certificate, the new certificate replaces the existing one. In the *Replace IF-MAP Certificate Confirmation* dialog box, click **Yes**.

### Generating Certificate Signing Requests

You can generate a CSR (certificate signing request) that you use to obtain a signed certificate from your own trusted CA. Once you receive the signed certificate, you can import it to the member, as described in *Uploading Certificates*.

To generate a CSR:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box, and then click **IF-MAP Client Certificate** -> **Create Signing Request** from the Toolbar.
2. In the **Create Certificate Signing Request** dialog box, enter the following:
   - **Secure Hash Algorithm and Key Size**: You can select SHA-1 and a RSA key size of 1024 or 2048. SHA-256 (SHA-2) can be selected together with a RSA key size of 2048 or 4096. The default value is SHA-256 2048.
   - **Common Name**: Specify the domain name of the member. You can enter the FQDN of the appliance.
   - **Organization**: Enter the name of your company.
   - **Organizational Unit**: Enter the name of your department.
   - **Locality**: Enter a location, such as the city or town of your company.
   - **State or Province**: Enter the state or province.
   - **Country Code**: Enter the two-letter code that identifies the country, such as US.
   - **Admin E-mail Address**: Enter the email address of the appliance administrator.
   - **Comment**: Enter information about the certificate.
3. Click **OK**.

### Uploading Certificates

When you receive the certificate from the CA, the appliance finds the matching CSR and takes the private key associated with the CSR and associates it with the newly imported certificate. The appliance then automatically deletes the CSR.

To import a certificate:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box, and then click **IF-MAP Client Certificate** -> **Upload Certificate** from the Toolbar.
2. Navigate to where the certificate is located and click **Open**.
3. If the appliance already has an existing IF-MAP client certificate, the new certificate replaces the existing one. In the *Replace IF-MAP Certificate Confirmation* dialog box, click **Yes**.

### Downloading Certificates

You can download the current certificate or a self-signed certificate. To download a certificate:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box, and then click **IF-MAP Client Certificate** -> **Download Certificate** from the Toolbar.
2. Navigate to where you want to save the certificate, enter the file name, and then click **Save**.

### Overriding IF-MAP Publishing Settings

When you enable IF-MAP publishing at the Grid level, all members, networks (IPv4 and IPv6), and DHCP ranges (IPv4 only) in the Grid inherit the same setting. To control which ip-mac and ip-duid metadata is published for specific leases that belong to a specific network or address range, you can override the Grid settings at a specific member, network, or range level. Note that you must first enable the IF-MAP service at the Grid and member levels in order to enable or disable IF-MAP publishing at other levels. For example, if you want the DHCP server to publish IF-MAP data for specific leases in a specific network that is served by a specific member, you must first enable the IF-MAP service at the Grid and member levels, as described in *Configuring a Grid to Support IF-MAP*. Then, you can enable IF-MAP publishing at the range level, as described in this section.

Though you can configure and save the settings of IF-MAP publishing any time at any level, the publishing does not actually happen unless the IF-MAP service is enabled at the Grid or member level. If a network or DHCP range is served by a specific member and you want to enable IF-MAP publishing for the network or range, you must first enable the IF-MAP service for the specified member.

To override IF-MAP publishing settings:

1. **Member**: From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box, and then click the Edit icon.
1. From the Data Management tab, select the DHCP tab -> Networks tab -> network check box, and then click the Edit icon.

2. In the editor, click Toggle Advanced Mode, and then click the IF-MAP tab.

3. Click Override and complete the following:
   - Enable IF-MAP Publishing: Select this check box to instruct the DHCP server to publish metadata to the IF-MAP server when the IF-MAP service is enabled for the Grid or member. Clear this check box so the DHCP server does not publish metadata to the server.

Deleting Data from the IF-MAP Server

The appliance allows you to delete IF-MAP data from the IF-MAP server. You can delete all IF-MAP data published by a specific member. You can also define how the IF-MAP server handles the deletion of existing metadata before the IF-MAP client publishes another update.

Deleting All Data

You can delete all IF-MAP data published by a specified member. To delete data published by all members in a Grid, you must delete data for each member individually.

To delete IF-MAP data published by a member from the IF-MAP database:

1. From the Data Management tab, select the DHCP tab -> Members tab, and then click Clear -> IF-MAP Data from the Toolbar.
2. In the Purge IF-MAP Data dialog box, click Select Member to select a member. If there are multiple members, Grid Manager displays the Member Selector dialog box from which you can select one. Click the member name in the dialog box, and then click Purge to delete all the DHCP data published by the Grid member. You can also click Clear to clear the displayed member and select a new one.

Deleting Existing Data Before Publishing

You can define how the IF-MAP server deletes existing metadata before an IF-MAP client publishes new data. You can configure the IF-MAP client to instruct the server to always delete existing data, never delete it, or delete the data before a specified time period.

To define how the IF-MAP server deletes DHCP data before the next publish:

1. From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
2. In the Grid DHCP Properties editor, click Toggle Advanced Mode.
3. Click the IF-MAP tab and complete the following:
   - Enable IF-MAP: Select this check box to enable the IF-MAP service.
   - Delete existing metadata: You can define how the IF-MAP server deletes the existing metadata before the IF-MAP client publishes new data. Select one of the following:
     - Always delete: Select this to always delete existing metadata before the IF-MAP client publishes updates. This is the default.
     - Do not delete: Select this to never delete the existing metadata before the IF-MAP client publishes updates.
     - Earlier than: Select this to delete metadata that was published before a given time before the IF-MAP client publishes updates. When you select this option, enter a time value, and then select a time unit from the drop-down list.
4. Save the configuration and click Restart if it appears if it appears at the top of the screen.

Starting DHCP Services on a Member

The DHCP service is disabled by default. After you complete the DHCP configuration, you can start DHCP service on a member. To enable the member to provide DHCPv6 service as well, you must start the DHCP service and then enable the DHCPv6 service on the member. In addition, you must specify the DHCP Unique Identifier (DUID) of the member. IPv6 clients use DUIDs to identify the source of the DHCP messages from servers.

To start DHCP service on a member:

1. From the Data Management tab, select the DHCP tab -> Members tab -> member check box.
2. Expand the Toolbar and click Start.
3. In the Start Member DHCP Service dialog box, click Yes.
4. Grid Manager starts DHCP on the selected member.

You can stop DHCP service on a member by selecting the member check box and click Stop from the Toolbar. This will stop DHCP service enabled on the LAN port.

To stop DHCP service enabled on the LAN2 port:

1. From the Data Management tab, select the DHCP tab -> Members tab -> member check box.
2. Click the Edit icon.
3. In the Member DHCP Properties editor, select the General tab.
4. Clear the check box for LAN2 under DHCP interfaces.
5. Save the configuration.
To enable DHCPv6 service on the member:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box.
2. In the **Member DHCP Properties** editor, select the **General Basic** tab.
3. In the **IPv6 Properties** section, do the following:
   - **Server DUID**: Enter the DUID of the member.
   - **Enable DHCPv6 Service**: Select this check box.
4. Save the configuration.

### Viewing DHCP Member Status

You can view DHCP member status after you configure DHCP properties and start or stop DHCP services on a member. To view member status:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **Members** section.
2. Grid Manager displays the following information:
   - **Name**: The name of the Grid member.
   - **Status**: The status of the DHCP services on the member. This can be one of the following:
     - **Not Running**: DHCP services have not been started on the member.
     - **Running**: The DHCP services are running properly on the member.
     - **Warning**: The member is connecting or synchronizing with its Grid Master.
     - **Error**: The member is offline, is not licensed (that is, it does not have a DNSone license with the Grid upgrade that permits Grid membership), is upgrading or downgrading, or is shutting down.
   - **Comment**: The information you entered for the member.
   - **IPv4 DHCP Utilization**: The percentage of the total IPv4 DHCP utilization of the member. This is the percentage of the total number of DHCP hosts, fixed addresses, reservations, and leases assigned to the member versus the total number of IP addresses (excluding IP addresses in the exclusion range) and all DHCP objects assigned to the member. Note that only enabled objects are included in the calculation. It does not include abandoned addresses or leases. The appliance updates the utilization data every 15 minutes. The appliance displays the utilization data in one of the following colors:
     - **Red**: The DHCP resources are 100% utilized.
     - **Yellow**: The utilization percentage is over the effective high watermark threshold.
     - **Blue**: The utilization percentage is below the effective low watermark threshold.
     - **Black**: The utilization percentage is at any number other than 100%, or within the effective thresholds.
   - **Site**: The site to which the member belongs. This is one of the predefined extensible attributes.

You can select the following additional columns for display:

- **Address**: The IP address of the member.
- **Static Addresses**: The number of static IP addresses.
- **Dynamic Addresses**: The number of dynamically assigned IP addresses.
- **IF-MAP Connection**: The status of the IF-MAP service connection on the member. This can be one of the following.
  - **Stopped**: The DHCP or IF-MAP service on the member is stopped, or the IF-MAP service is not enabled.
  - **Running**: The IF-MAP client is connected to the IF-MAP server and the IF-MAP service is running properly.
  - **Failed**: The IF-MAP client cannot publish data to the IF-MAP server due to some errors.
  - **Warning**: Some non-fatal errors occurred. The IF-MAP client attempts to reconnect to the server.

**Note**: You can mouse over on the informational icon next to the status to view detailed information, including the status description and the timestamp when the status initially changed.

- **IF-MAP Last Update**: The timestamp the status of the IF-MAP service was last updated. For example, if the IF-MAP connection status is **Running** and this field shows 2011-11-20 12:30:42 EST, it means that an IF-MAP operation, such as a publish, was last completed on November 20, 2011 at 12:30:42 Eastern Standard Time.

To view status information about the IF-MAP connection on an independent appliance, from the **Data Management** tab -> **DHCP** tab, click **System DHCP Properties** from the toolbar. The appliance displays the following:

- **IF-MAP Connection**: The status of the IF-MAP service on the independent appliance. A color icon associated with the connection status appears before the status.
- **IF-MAP Connection Information**: Detailed information about the status. On a Grid member, this information appears when you mouse over on the informational icon.
- **IF-MAP Last Update**: The timestamp when the status of the IF-MAP service last changed.

**Note**: For more information about these fields, see descriptions about Grid member status in this section.

You can view detailed information about a specific member by clicking the member link. Grid Manager displays the following information about the selected member.
• **Network**: The network assigned to the member.
• **Comment**: The information about the network.
• **IPv4 DHCP Utilization**: The percentage of the DHCP usage of the network. This is the percentage of the total number of fixed addresses, reservations, hosts, and active leases on the network over the total IP addresses in the range, excluding the number of addresses on the network. Note that only enabled objects are included in the calculation. It does not include abandoned addresses or leases.
• **Site**: The site to which the DHCP object belongs. This is one of the predefined extensible attributes. In the member panel, you can select the following additional fields for display:
• **Disabled**: Indicates whether the member is disabled or not.
• **IPAM Utilization**: When you define a network, this is the percentage based on the IP addresses in use divided by the total addresses in the network. For example, in a /24 network, if there are 25 static IP addresses defined and a DHCP range that includes 100 addresses, the total number of IP addresses in use is 125. Of the possible 256 addresses in the network, the IPAM utilization is about 50% for this network.

When you define a network container that contains subnets, this is the percentage of the total address space defined within the container regardless of whether any of the IP addresses in the subnets are in use. For example, when you define a /16 network and then 64 /24 networks underneath it, the /16 network container is considered 25% utilized even when none of the IP addresses in the /24 networks is in use.

You can use this information to verify if there is a sufficient number of available addresses in a network. The IPAM utilization is calculated approximately every 15 minutes.

• Extensible attributes that associate with the network.

You can also sort the data in ascending or descending order by column. For information, see *Customizing Tables*.

**Viewing DHCP Configuration Files**

You can view the IPv4 and IPv6 DHCP configuration of a selected member. The format of the configuration file depends on the browser you use. To view the DHCP configuration of a selected member:

1. From the **Data Management** tab, select the **DHCP** tab - > **Members** tab - > **Members** - > **member** check box.
2. Expand the **Toolbar**, select **View DHCP Configuration**, and then select either **IPv4** or **IPv6**. Grid Manager displays the IPv4 or IPv6 DHCP configuration of the selected member in a new browser. You can print and save the file using the corresponding functions in your browser.

**Chapter 27 Managing IPv4 DHCP Data**

This chapter explains how to configure and manage IPv4 DHCP data. It contains the following sections:

- **Configuring DHCP for IPv4**
- **About the Next Available Network or IP Address**
  - Obtaining the Next Available
  - Guidelines for the Next Available Network and IP Address
- **Configuring IPv4 Networks**
  - Adding IPv4 Networks
  - Viewing Networks
  - Modifying IPv4 Networks
  - Deleting IPv4 Networks
- **Configuring IPv4 Shared Networks**
  - Adding IPv4 Shared Networks
  - Viewing Shared Networks
  - Modifying IPv4 Shared Networks
  - Deleting IPv4 Shared Networks
- **Configuring IPv4 Address Ranges**
  - Adding IPv4 Address Ranges
  - Modifying IPv4 Address Ranges
  - Controlling Lease Assignments
  - Deleting IPv4 Address Ranges
- **Configuring IPv4 Fixed Addresses**
  - Adding IPv4 Fixed Addresses
  - Modifying IPv4 Fixed Addresses
  - Deleting Fixed Addresses
- **Configuring IPv4 Reservations**
  - Adding IPv4 Reservations
  - Modifying IPv4 Reservations
- **Viewing IPv4 DHCP Objects**
- **About Roaming Hosts**
  - Configuring Roaming Hosts
  - Enabling Support for Roaming Hosts
  - Adding IPv4 Roaming Hosts
• Adding IPv6 Roaming Hosts
• Adding IPv4/IPv6 Roaming Hosts
• Viewing Roaming Hosts
• Setting Properties for Roaming Hosts
• Deleting Roaming Hosts

Configuring DHCP for IPv4

To configure DHCP service for an IPv4 network and the resources in the network, perform the following tasks:

1. Create a network and assign it to Grid members or Microsoft DHCP servers, or an interface on an external discovered device. For information, see Adding IPv4 Networks and Modifying IPv4 Networks.
2. Configure DHCP properties for the network. You can override properties set at the Grid or member level and enter unique values for the network. For information, see Configuring General IPv4 DHCP Properties and Configuring DHCP IPv4 and IPv6 Common Properties.
3. Optionally, assign zones to a network. For information, see Associating Networks with Zones.
4. Add a DHCP range to the network and assign it to a member, a failover association, or a Microsoft DHCP server. For information, see Adding IPv4 Address Ranges and Modifying IPv4 Address Ranges.
5. Optionally, add exclusions to the DHCP range for addresses that are not used for dynamic allocation. For information, see Configuring IPv4 Fixed Addresses.
6. Optionally, configure DHCP properties for the address range. You can override properties set at an upper level and enter unique values for the address range. For information, see Modifying IPv4 Address Ranges.
7. Optionally, define filters for precise address assignments and apply them to the DHCP range. For information, see About IPv4 DHCP Filters.
8. Optionally, add fixed addresses and reservations to the network and configure DHCP properties for them. For information, see Configuring IPv4 Fixed Addresses and Configuring IPv4 Reservations.

About the Next Available Network or IP Address

When you create certain objects through Grid Manager, the appliance can obtain the next available IPv4 or IPv6 network from a specific network container. It can also obtain the next available IP address from a specific network or address range. This feature automates the allocation of networks and IP addresses so you can manage your network space more efficiently. You can also use this feature to organize network devices. For example, you can create a reserved range called “Printer Range” to reserve static IP addresses for printers in your network. When you allocate IP addresses for printers, you can have the appliance search for the next available IP address within “Printer Range,” and then allocate the next available address to a new printer.

When you create a new network, the appliance can look up the next available network address within a specific network container. The next available network address is the first unused network address in the network container to which you have administrative permissions. For information about creating IPv4 and IPv6 networks using the next available feature, see Adding IPv4 Networks and Adding IPv6 Networks. You can also obtain the next available IP address when you define a fixed address, reservation, or host record. The next available IP address is the first unused IP address in a specified network, DHCP range, or reserved range to which you have administrative permissions. For information about creating fixed addresses, reservations, and host records using the next available feature, see Configuring IPv4 Fixed Addresses, Configuring IPv4 Reservations, and Adding Host Records.

Obtaining the Next Available

The appliance searches for the next available network or IP address based on the context you define when you create an object. For example, when you create a network within a specific network container, the appliance searches for the next available network within the specified container. Similarly, when you drill down to an address range and create an object from there, the appliance looks up the next available IP address within that address range. If you are not within a specific network or address range when you create an object, Grid Manager displays a selector from which you can select the network or address range for the next available network or IP address.

For information about how the appliance select the next available network and IP address, see Guidelines for the Next Available Network and IP Address.

Guidelines for the Next Available Network and IP Address

The appliance follows certain rules when searching for the next available network and IP address in the specified wizard, network container, and address range.

In a wizard where you can obtain the next available network or IP address, the following applies:

• In a wizard, if you add a network or IP address and then delete it, the appliance excludes it from the next available. When you try to obtain the next available network or IP address in the same wizard, the appliance does not return the deleted network or IP address until you exit the wizard.

In a network, the appliance searches for the next IP address that meets all of the following criteria:

• It does not match any DNS resource record, such as an A or PTR record, that is associated with an IP address.
• It is not assigned to a DHCP fixed address or host address record.
Adding IPv4 Networks

When you configure an IPv4 network, you must assign either Grid members or Microsoft servers to the network. A network cannot be served by a mix of Microsoft and Infoblox DHCP servers. Multiple servers can serve a network, but Grid members and Microsoft servers cannot serve the same network.

A Grid member can serve only one network view. Similarly, a Microsoft server can serve only one network view. Therefore when you assign Grid members to networks, you must assign the members to networks in the same network view. For information, see Configuring DHCP for IPv4.

If you have enabled support for RIR (Regional Internet Registry) updates and are adding an RIR IPv4 network container or network to NIOS, Grid Manager displays an RIR section in the Add IPv4 Network wizard. You must enter RIR related information in this section in order for NIOS to associate the newly added network with an RIR organization. For more information about RIR address allocation and updates, see RIR Registration Updates.

To add an IPv4 network:

1. From the Data Management tab, select the DHCP tab -> Networks tab.
2. In the Networks section, select IPv4 Network from the Add drop-down menu.
3. In the Add Network wizard, select one of the following and click Next:
   - Add Network: Click this to add a network from scratch.
   - Add Network using Template: To use a template, click this, and then click Select Template and select a network template. For information, see About IPv4 Network Templates. You can also create an IPv4 network from the Tasks Dashboard, as described in The Tasks Dashboard.
4. Complete the following and click Next:
   - Regional Internet Registry: This section appears only when support for RIR updates is enabled. For information about RIR, see RIR Registration Updates. Complete the following to create an RIR IPv4 network container or network:
     - Internet Registry: Select the RIR from the drop-down list. The default is RIPE. When you select None, the network is not associated with an RIR organization.
     - Organization ID: Click Select Organization and select an organization from the RIROrganizationSelector dialog box.
     - Registration Status: The default is Not Registered. When adding an RIR allocated network, you can change this to Registered and select the Do not update registrations check box below. Note that when you select API as the communication method, the registration status will be updated automatically after the registration update is completed. However, when you select Email as the communication method, the registration status will not be automatically updated. If you are creating a new network and the registration update is completed successfully, the status will be
changed to Registered. If the update fails, the status will be changed to Not Registered. The updated status and timestamp are displayed in the Status of last update field in the IPv4 Network Container or IPv4 Network editor.

- **Registration Action**: Select the registration action from the drop-down list. When you select Create, the appliance creates the IPv4 network and assigns it to the selected organization. When you select None, the appliance does not send registration updates to RIPE. If you are adding an existing RIR allocated network to NIOS, select None. When you are adding networks to an RIR allocated network (a parent network), select Create. Ensure that the parent network associated with an RIR organization already exists.

- **Do not update registrations**: Select this check box if you do not want the appliance to submit RIR updates to RIPE. By default, the appliance sends updates to the RIR database based on the configured communication method.

- **Network View**: This appears only when you have multiple network views. From the drop-down list, select the network view in which you want to create the network.

- **Netmask**: Enter the netmask or use the netmask slider to select the appropriate number of subnet mask bits for the network. The appliance supports /1 to /32 netmasks. Note that when you use a template that contains a fixed netmask, you cannot adjust the netmask for this network. Microsoft servers can serve networks with /1 to /31 netmasks. Infoblox DHCP servers can serve networks with /8 to /32 netmasks.

- **Note**: Since Infoblox DHCP servers do not support /1 to /7 networks, you can assign these networks to Microsoft DHCP servers only. You can create DHCP ranges and fixed addresses within these subnets.

- **Networks**: Do one of the following to add new networks:
  - Click the Add icon to enter a new network. Grid Manager adds a row to the table. Enter the network address in the Network field. Click the Add icon again to add another network.
  - or
  - Click the Next Available icon to have the appliance search for the next available network. Complete the following in the Next Available Networks section:
    - **Create new network(s) under**: Enter the network container in which you want to create the new network. When you enter a network that does not exist, the appliance adds it as a network container. When you enter a network that is part of a parent network, the parent network is converted into a network container if it does not have a member assignment or does not contain address ranges, fixed addresses, reservations, shared networks, and host records that are served by DHCP. When you enter a network that has a lower CIDR than an existing network, the appliance creates the network as a parent network and displays a message indicating that the newly created network overlaps an existing network. You can also click Select Network to select a specific network in the Network Selector dialog box. For information about how the appliance searches for the next available network, see Obtaining the Next Available.
    - **Number of new networks**: Enter the number of networks you want to add to the selected network container. Note that if there is not enough network space in the selected network to create the number of networks specified here, Grid Manager displays an error message. The maximum number is 20 at a time. Note that when you have existing networks in the table and you select one, the number you enter here includes the selected network.
    - **Click Add Next** to add the networks. Grid Manager lists the networks in the table. You can click Cancel to reset the values.

**Note**: You must click Add Next to add the network container you enter in the Next Available Networks section. If you enter a network in the Next Available Networks section and then use the Add icon to add another network, the appliance does not save the network you enter in the Next Available Networks section until you click Add Next.

- **Comment**: Enter useful information about the network, such as the name of the organization it serves.

- **The Sync to MGM drop-down list is available only on the managed Grid when it remains joined with the Multi-Grid Master. Select one of the following from the Sync to MGM drop-down list:**
  - **Yes**: Select this to enable synchronization of networks between the managed Grid and Multi-Grid Master.
  - **No**: Select this to disable synchronization of networks between the managed Grid and Multi-Grid Master.

**Note**: If you have selected No at the parent network (disabled synchronization) and if you try to select Yes when adding a child network, the appliance returns an error. This means that you cannot override the settings at the child level if you have already restricted synchronization at the parent network.

- **Use Inherited Setting**: Select this to inherit synchronization settings from the parent object.

- **Automatically Create Reverse-Mapping Zone**: This function is enabled if the netmask of the network equals /8, /16, or /24. Select this to have the appliance automatically create reverse-mapping zones for the network. A reverse-mapping zone is an area of network space for which one or more name servers have the responsibility for responding to address-to-name queries. These zones are created in the DNS view assigned to receive dynamic DNS updates at the network view level.

- **Disable for DHCP**: Select this if you do not want the DHCP server to provide DHCP services for this network at this time. This feature is useful when you are in the process of setting up the DHCP server. Clear this after you have configured the server and are ready to have it serve DHCP for this network.

The Cloud section appears when the Cloud Network Automation license is installed on the Grid Master. For information, see Deploying Cloud Network Automation. To delegate authority for this network, complete the following:

**Delegate authority from the Grid Master**

- **Delegate To**: This field indicates whether the authority for the network you want to create has already been delegated to a Cloud Platform Appliance. Click Select to choose the Cloud Platform Appliance to which you want to delegate authority. The Member Selector displays only Cloud Platform Appliances in the Grid. Click the member, and Grid Manager displays the member name next to this field.
This cloud member now assumes authority for this network, and the Grid Master does not have authority any more. You can also click Clear to remove authority delegation from the selected Cloud Platform Appliance and return authority back to the Grid Master.

5. Click Next and add a Grid member or Microsoft server as a DHCP server for the network. A network can be served by either Grid members or Microsoft servers, but not both at the same time.

- Click the Add icon and select one of the following options:
  - **Add Infoblox Member**: Select this option to add a Grid member as a DHCP server for the network. Select the Grid member from the Member Selector dialog box. Keep in mind, DHCP properties for the network are inherited from this member. The network can be served by multiple members, but a member can serve networks in one network view only.

  or

  - **Add Microsoft Server**: Select this option to add a Microsoft server as a DHCP server for the network. Select the Microsoft server from the Microsoft Server Selector dialog box.

6. Click Next to associate Active Directory Sites with the network. For more information, see Associating Active Directory Sites with Networks.

7. Click Next to override DHCP properties as described in About DHCP Properties. This only applies if you are adding a network that is served by an Infoblox Grid member.

8. (Applies only with Network Insight) Click Next to initiate or disable discovery of the new network(s). This step is not required for creating a new network. Discovery settings differ based on whether you are defining one network or multiple networks.

- **Configuring one network**: discovery settings include the following: Enable Discovery and Enable Immediate Discovery, selecting a Probe member to perform the discovery; and Polling Options, which define how the network will be discovered by the Probe member, including the ability to enable or disable the use of SNMP Credentials and CLI Credentials, along with Switch Port Data Collection settings. By default, all Polling Options discovery settings are inherited from the parent network (or Grid, if no parent exists) unless you click Override. Polling Options govern the protocols used to query and collect information about the network devices being discovered. For more information, see the section Configuring Discovery Properties for a complete description of discovery Polling Options.

  or

- **Configuring more than one network**: If the networks are child networks, they automatically inherit the settings of the parent network, including discovery settings and the discovery member. Discovery is disabled for any parent networks. These settings will not appear in the wizard page. For discovery of multiple networks, you can only enable or disable Immediate Discovery.

9. As part of creating a network in IPAM or DHCP, you can provision the network on an actual device (switch, router, or switch-router), that is discovered and managed through the Grid Manager.

- Begin by checking the Enable Network Provisioning check box, and clicking the Select Device button. Choose your device from the Device Selector dialog. (Click Clear to remove the setting. For more information, see the section Using the Device Selector.)

- If you performed DHCP configuration in the previous step of the Add Network Wizard, the Router IP value will automatically be populated with the DHCP Router IP address value. Otherwise, you enter the standard router IP address value (for example, if Grid Manager discovers and manages a router 172.16.22.1, the IP value 172.16.22.1 should be entered in the Router IP field).

- If required for the newly provisioned network to ensure that attached devices receive DHCP auto-configuration, enable the DHCP Forwarding check box. For this setting, if a DHCP Failover was previously configured, the IP addresses defined for DHCP failover are automatically used for the DHCP forwarding configuration.

- You will also need to choose an interface on the selected device on which to provision the network by selecting it from the Interface drop-down menu. Grid Manager ensures that only those interfaces that can support provisioning, and are available for provisioning (that do not have an Operation Status of Up), appear in the drop-down menu.

- Otherwise, when creating networks and provisioning them on managed devices, you can create a VLAN on which to provision the network by clicking the Create VLAN option and entering the VLAN Name and VLAN ID. Ensure that the VLAN ID value you enter is appropriate for the application - do not create a new VLAN and provision a network for a VLAN value that is already actively carrying traffic for another routing domain.

  If a selected device does not support VLANs, the Create VLAN option will not appear.

10. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see About Extensible Attributes.

If you are adding an RIR network, the RIR network attribute table appears. For information about these attributes and how to enter them, see RIR Network Attributes. You can preview the information before the appliance submits updates to the RIPE database. To preview registration updates, click Preview RIR Submissions. For more information, see Previewing Registration Updates.

**Note**: You cannot leave an optional RIR attribute value empty. If you do not have a value for an RIR attribute, you must delete it from the table. You can enter up to 256 characters for all RIR attributes.

11. As the final step in the Add IPv4 Network wizard, you define when Grid Manager provisions the new network by scheduling it. You also schedule when the associated port control task executes (if a port configuration has been specified).
To create the new network and its associated port configuration immediately, select Now. Grid Manager synchronizes the port control task to take place at the same time as the creation of the new network.

You can choose to have Grid Manager execute the port control task at the same time as the network creation. To do so, select a specific time.

You can choose to have Grid Manager execute the port control task at a later time by selecting Later.

Choose a Selected time by entering or selecting a Start Date (click the calendar icon to choose a calendar date) and a Start Time, and choose a Time Zone.

12. Choose one of the following from the Save & ... drop-down button menu:

- Click Save & Close to add the new network and close the wizard (this is the default).
- Click Save & Edit to add the new network and launch the editor.
- Click Save & New to add the new network and launch the wizard again to add another network.

Note: At any step during the wizard, you can click Schedule for Later to schedule the task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

After you create a network, you can do the following:

- Use the split network feature to create subnets for the network. For information, see Splitting IPv4 Networks into Subnets.
- Use the join networks feature to create a parent network that encompasses multiple subnets into a larger network. For information, see Joining IPv4 Networks. You can also create a shared network for subnets that are on the same network segment.

Networks served by Microsoft servers do not support the split and join functions.

Viewing Networks

You can view IPv4 networks from the IPAM tab -> Net Map and List panels. The Net Map panel provides a graphical view of your networks and the List panel displays the networks in table format. For more information, see IPv4 Network Map and IPAM Home.

You can also view a list of IPv4 and IPv6 networks in the DHCP tab -> Networks tab -> Networks panel. This panel displays all IPv4 and IPv6 networks.

In any of these panels, you can use filters or the Go to function to navigate to a specific network. You can also create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters. You can add, delete, or edit a network. You can also monitor the DHCP utilization of a selected network.

When viewing networks, you can choose to view them in one of the following views:

- Click Toggle Hierarchical View to view networks hierarchically in a parent-child structure (networks in a network container). You can view detailed information about the networks by clicking the network link and drilling down to the lowest hierarchical level, and then opening a network. To go back to a previous hierarchical view, click the link of the corresponding level in the breadcrumb. The hierarchical view is the default view.
- Click Toggle Flat View to display a flat list of all networks and network containers. The parent and child networks are listed separately in the flat view.

Depending on where you view your networks from, Grid Manager displays some of the following information by default. You can also select specific information for display.

- **Network**: The network address.

  The network is displayed in one of the following colors:

  - **Yellow**: The network is unmanaged.
  - **Blue**: The selected network.
  - **Gray**: The network is currently not available as a NIOS network object.
  - **Comment**: The information you entered about the network.
  - **IPAM Utilization**: This information is available for IPv4 networks only. It displays the percentage based on the IP addresses in use divided by the total addresses in the network. For example, in a /24 network, if there are 25 static IP addresses defined and a DHCP range that includes 100 addresses, the total number of IP addresses in use is 125. Of the possible 256 addresses in the network, the IPAM utilization is about 50% for this network. The appliance updates the IPAM utilization data immediately for a network container, but for a network it is updated every 15 minutes. The IPAM utilization data is displayed in one of the following colors:
    - **Red**: The IPAM utilization percentage is above the configured Trigger value.
    - **Blue**: The IPAM utilization percentage is below the configured Trigger value.
  - **Site**: The site to which the network belongs. This is one of the predefined extensible attributes.
  - **Protocol**: Displays whether the network is an IPv4 or IPv6 network.
  - **Disabled**: Indicates if the network is disabled.
  - **Leaf Network**: Indicates whether the network is a leaf network or not. A leaf network is a network that does not contain other networks.
  - **IPv4 DHCP Utilization**: This information is available for IPv4 networks only. It displays the percentage of the total DHCP usage of theIPv4 network. This is the percentage of the total number of DHCP hosts, fixed addresses, reservations, and active leases in the...
The DHCP resources are 100% utilized.

Network
Parent: The IP address of a DHCP object, such as a DHCP range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address. For a DHCP range, this field displays the start and end addresses of the range. For a host that has multiple IP addresses, each IP address is displayed separately. Note that the appliance highlights all disabled DHCP objects in gray.

You see the following when RIR is enabled (For information, see RIR Registration Updates):

- **RIR Organization**: This appears only if support for RIR updates is enabled. This displays the name of the RIR organization to which the network is assigned.
- **RIR Organization ID**: This appears only if support for RIR updates is enabled. This displays the ID of the RIR organization to which the network is assigned.
- **RIR Registration Status**: This appears only if support for RIR update is enabled. This field displays the RIR registration status. This can be **Registered** or **Not Registered**. **Registered** indicates that the network has a corresponding entry in the RIPE database.
- **Last Registration Updated**: Displays the timestamp when the last registration was updated. The displayed timestamp reflects the timestamp used on the Grid Master.
- **Status of Last Registration Update**: Displays the registration status and communication method of the last registration update. The status can be Pending, Sent, Succeeded, or Failed. Each time you send a registration update to create, modify, or delete a network container or network, the updated status will be displayed here. If you have selected not to send registration updates, the previous status is retained.

You see the following only with Network Insight (For information, see Infoblox Network Insight):

- **Discovery Enabled**: Indicates whether discovery is allowed on the network container or the network.
- **Managed**: Indicates whether the network is set to Managed status under NIOS.
- **FirstDiscovered**: The date and timestamp of the first occasion that NIOS discovered the network.
- **LastDiscovered**: The date and timestamp of the last occasion that NIOS performed discovery on the network.

You see the following when the Cloud Network Automation license is installed on the Grid Master (For information, see Deploying Cloud Network Automation):

- **Cloud Usage**: This field indicates whether this object is associated with any specific cloud extensible attributes or within a scope of delegation. It can be one of the following:
  - **Cloud from adapter**: Indicates that this object has been created by a cloud adapter and it may or may not be within a scope of delegation at the moment.
  - **Cloud from delegation**: Indicates that this object is within the scope of delegation or the object itself defines a scope of authority delegation, and it is not created by a cloud adapter.
  - **Used by cloud**: Indicates that this network or network container is associated with the extensible attribute **Is External** or **Is Shared** and the value is set to True, which implies the network is a private or shared network managed by the CMP, and it is not Cloud from adapter or Cloud from delegation.
  - **Non-cloud**: The object is a regular NIOS object and is not within the scope of any authority delegation nor is it associated with any of these extensible attributes: Cloud API Owned, Is External, or Is Shared. NIOS admin users can modify this object based on their permissions.
- **Owned By**: A cloud object can be owned by the Grid Master or the cloud adapter. When the object is created by the Cloud Platform member, this shows Grid. If the object is created by the cloud adapter, this shows Adapter.
- **Delegated To**: This tells you whether a cloud object has been delegated to a Cloud Platform Appliance or not. If the cloud object has a parent object and the parent has been delegated, this field shows the parent delegation and you cannot modify the field.
- **Extensible attributes (Building, Country, Region, State, and VLAN)**: You can select the extensible attributes such as Building, Country, Region, State, and VLAN for display. When you enable other features such as RIR, Network Insight, and Cloud Network Automation, you can select additional attributes for display.

You can sort the list of networks in ascending or descending order by certain columns. For information about customizing tables in Grid Manager, see Customizing Tables.

You can also modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables. You can edit values of inheritable extensible attributes by double clicking on the respective row. If an extensible attribute has an inherited value, then the cell is highlighted in blue when you perform an inline editing. The Descendant Actions dialog box is displayed when you click Save. For information, see Managing Inheritable Extensible Attributes at the Parent and Descendant Level. If you delete the value of an inheritable extensible attribute at the parent level, you can choose to preserve the descendant value or remove it. For information, see Deleting Inheritable Extensible Attributes Associated with Parent Objects.

Viewing Network Details

You can view detailed information about a specific network by clicking the network link. Grid Manager displays the objects in the network, including DHCP ranges, hosts, fixed addresses and roaming hosts. It displays the following information about the network:

- **IPAddress**: The IP address of a DHCP object, such as a DHCP range, fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address. For a DHCP range, this field displays the start and end addresses of the range. For a host that has multiple IP addresses, each IP address is displayed separately. Note that the appliance highlights all disabled DHCP objects in gray.
The IP address is displayed in one of the following colors:
- **Yellow:** The IP address is unmanaged.
- **Blue:** The IP address is excluded.
- **Pink:** Indicates IP address conflicts.
- **Gray:** The IP address is currently not available as a NIOS object.

- **Type:** The DHCP object type, such as **DHCPRange** or **FixedAddress**.
- **Name:** The object name. For example, if the IP address belongs to a host record, this field displays the hostname.
- **Comment:** The information you entered for the object.
- **IPv4DHCPUtilization:** The percentage of the total DHCP usage of a DHCP range. This is the percentage of the total number of fixed addresses, reservations, hosts, and active leases in the DHCP range divided by the total IP addresses in the range, excluding the number of addresses in the exclusion ranges. Note that only enabled objects are included in the calculation. It does not include abandoned addresses or leases.
- **Site:** The site to which the DHCP object belongs. This is one of the predefined extensible attributes. You can select the following additional columns for display:
- **Static Addresses:** Indicates whether the IP address is a static address.
- **Dynamic Addresses:** Indicates whether the IP address is a dynamically assigned address.
- **Disabled:** Indicates whether the object is disabled.
- **Priority:** Displays the priority of a DHCP range when NAC filters are applied.
- **Available extensible attributes.

You can also do the following in this panel:

- **Modify some of the data in the table. Double click a row, and either modify the data in the field or select an item from a drop-down list. Click **Save** to save the changes. Note that some fields are read only. You can edit values of inheritable extensible attributes by double clicking on the respective row. If an extensible attribute has an inherited value, then the cell is highlighted in blue when you perform an inline editing. The **Descendant Actions** dialog box is displayed when you click **Save**. For information, see **Managing Inheritable Extensible Attributes at the Parent and Descendant Level**. If you delete the value of an inheritable extensible attribute at the parent level, you can choose to preserve the descendant value or remove it. For information, see **Deleting Inheritable Extensible Attributes Associated with Parent Objects**.
- **Sort the displayed data in ascending or descending order by column.**
- **Click Go to IPAM View** to view information about the object in the IPAM tab.
- **Add new objects, such as DHCP ranges, to the network.**
- **Delete or schedule the deletion of a selected object or multiple objects.**
- **Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.**
- **Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.**
- **Print or export the data.**

**Modifying IPv4 Networks**

You can modify existing network settings and override the Grid or member DHCP properties, with the exception of the network address and netmask.

To modify an IPv4 network:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network check box, and then click the Edit icon.
   or From the Data Management tab, select the IPAM tab -> network check box, and then click the Edit icon.
2. The IPv4 Network editor contains the following basic tabs from which you can modify data:
   - **Genera Basic:** You can modify the following fields:
     - **Comment:** The information you entered for the network.
     - **Disabled:** This field is displayed only if the selected network is a network without a child network under it. You can disable and enable existing networks instead of removing them from the database, if the selected network does not have a child subnet. This feature is especially helpful when you have to move or repair the server for a particular network.

### Restricting synchronization of a network

- **Disable sync to MGM:** Select this check box to disable synchronization of a network from the managed Grid to the Multi-Grid Master. This check box is available only on the managed Grid when it remains joined with the Multi-Grid Master.

When the Cloud Network Automation license is installed on the Grid Master, Grid Manager displays the following information in the Cloud section: **Cloud Usage, Owned By, and Delegated To.** You cannot modify these fields. For more information, see Viewing Networks.

- **Member Assignment:** Add or delete a Grid member that provides DHCP services for this network. For information, see Adding IPv4 Networks.
- **IPv4DHCPOptions:** Keep or delete the inherited DHCP properties or override them and enter unique settings for the network. For information, see Defining IPv4 DHCP Options.
- **Discovery:** Checking the Enable Discovery check box informs NIOS to begin discovering the network after you click **Save and Close.** You manage discovery polling settings local to each network from this page. For a complete overview of features on this page, see Discovering Devices and Networks and its subsections.
• **Discovery Exclusions:** IP Addresses and IP ranges can be locally excluded from discovery by clicking the Add icon and selecting **Add IP Address or Add IP Range**. These IP addresses or IP ranges are selected from within the chosen network. For related information, see **Excluding IP Addresses from Discovery** and its subsections.

• **Discovery Blackout:** Define extended time periods and regularly scheduled times when discovery and/or Port Configuration tasks will not take place on a network. Editing a network under DHCP, blackout settings apply only to the specified network. You also specify the scheduled time when the blackout period begins, and the duration of the blackout period. By default, the network inherits its discovery blackout settings from the Grid level. For related information, see **Defining Blackout Periods** and its subsections.

**Note:** Discovery blackout settings also can be defined for DHCP ranges.

- **RIR Registration:** Modify RIR network information. This tab appears only when support for RIR updates is enabled. For information, see **Modifying RIR Network Data**.
- **Extensible Attributes:** Add and delete extensible attributes that are associated with a specific network. You can also modify the values of the extensible attributes. For information, see **About Extensible Attributes**. You can edit values of inheritable extensible attributes by double clicking on the respective column. If an extensible attribute has an inherited value, then the cell is highlighted in blue when you perform an inline editing. The **Descendant Actions** dialog box is displayed when you click **Save**. For information, see **Managing Inheritable Extensible Attributes at the Parent and Descendant Level**. If you delete the value of an inheritable extensible attribute at the parent level, you can choose to preserve the descendant value or remove it. For information, see **Deleting Inheritable Extensible Attributes Associated with Parent Objects**.
- **Permissions:** This tab appears only if you belong to a superuser admin group. For information, see **Managing Permissions**.

3. Optionally, click **Toggle Advanced Mode** to display the following tabs from which you can modify advanced data.

- **General Advanced:** You can associate zones with a network. For information, see **Associating Networks with Zones**.
- **IPv4 DDNS:** Keep the inherited DDNS settings or override them and enter unique settings for the network. Note that you must click **Override** and select **Enable DDN Supdates** for the DDNS settings you configure in this tab to take effect. For information, see **Enabling DDNS for IPv4 and IPv6 DHCP Clients**.
- **IPv4 BOOTP/PXE:** Keep the inherited BOOTP properties or override them and enter unique settings for the network. For information, see **Configuring IPv4 BOOTP and PXE Properties**.
- **IPv4 Filters:** You can keep the inherited IPv4 logic filters or override them and add a new IPv4 logic filter. For information, see **Applying Filters to DHCP Objects**.
- **IPv4 DHCP Thresholds:** Keep the inherited thresholds settings or override them and enter unique settings for the network. For information, see **Configuring Thresholds for DHCP Ranges**.

4. Save the configuration or click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Tasks**.

**Deleting IPv4 Networks**

When you delete a network, all of its data, including all DHCP records, subnets, and records in its subnets, is deleted from the database. Because of the potentially large loss of data that can occur when you delete a network, the appliance stores the deleted network in the Recycle Bin. You can restore a deleted network from the Recycle Bin, if enabled. You can also disable a network instead of deleting it. For information, see **Modifying IPv4 Networks**.

To delete a network:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** section -> **network** check box, and then select **Delete** or **Schedule Delete** from the Delete drop-down menu.
2. To delete the network now, in the **Delete Confirmation** dialog box, click **Yes**. To schedule the deletion, see **Scheduling Deletions**.

The appliance puts the deleted network in the Recycle Bin, if enabled.

Any Port reservation associated with the deleted network will also be deleted without user intervention.

**Configuring IPv4 Shared Networks**

You can combine individual contiguous networks into a shared network to allow the DHCP server to assign IP addresses from any subnet (that resides on the same network interface) in the shared network.

Before creating a shared network, you must first create the subnets. For example, you must first create the networks 10.32.1.0 and 10.30.0.0 before designating them to a shared network. For more information, see **About Shared Networks**

**Adding IPv4 Shared Networks**

To add a shared network:

1. Select the **Data Management** tab.
2. If you have more than one network view in the system, select the network view in which you want to add the network.
3. Select the **DHCP** tab -> **Networks** tab.
4. In the **Shared Networks** section, select **IPv4 Shared Network** from the Add drop-down menu.
5. In the **Add IPv4 Shared Network** wizard, complete the following and click **Next**.
• **Name:** Enter the name of the shared network.
• **Comment:** Enter information about the shared network.
• **Disabled:** Select this if you want to enable the shared network at a later time. You can disable and enable existing networks instead of removing them from the database. This feature is especially helpful when you have to move or repair the server for a particular network.

6. Do the following to add networks:
   a. Click the **Add** icon.
   b. In the **Select Network** dialog box, select the networks that you want to include in the shared network. Ensure that the networks are served by the same Grid members to avoid DHCP inconsistencies.

7. Click **Next** to configure or override DHCP options as described in **Defining IPv4 DHCP Options**.

8. Click **Next** to enter values for required extensible attributes or add optional extensible attributes for the shared network. For information, see **Using Extensible Attributes**.

9. Save the configuration or click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see **Scheduling Tasks**.

**Viewing Shared Networks**

To view IPv4 and IPv6 shared networks:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Shared Networks**.
2. Grid Manager displays the following information:
   • **Name:** The name of the shared network.
   • **Protocol:** Displays whether the network is an IPv4 or IPv6 network.
   • **Comment:** The information you entered about the shared network.
   • **IPv4 DHCP Utilization:** The percentage of the DHCP utilization of the networks that belong to the shared network. This is the percentage of the total number of available IP addresses from all the networks that belong to the shared network versus the total number of all IP addresses in all of the networks in the shared network.
   • **Site:** The site to which the shared network belongs. This is one of the predefined extensible attributes.

You can select **Disabled** or available extensible attributes for display. You also can view detailed information about a network in a shared network by clicking the network link.

In this panel, you can use filters or the **Go to** function to navigate to a specific network. You can also create a quick filter to save frequently used filter criteria. For information, see **Using Quick Filters**.

You can sort the list of networks in ascending or descending order by columns. For information about customizing tables in Grid Manager, see **Customizing Tables**.

You can also modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see **Modifying Data in Tables**.

**Modifying IPv4 Shared Networks**

You can modify existing network settings and override the Grid or member DHCP properties:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Shared Networks** section -> **shared_network** check box, and then click the **Edit** icon.
2. The **Shared Network** editor contains the following tabs from which you can modify data:
   • **General:** Modify the fields **Name**, **Comments**, and **Disabled** as described in 4823774
   • **Networks:** Displays the networks that are currently assigned to the shared network. You can add or delete a network. To add a network, click the **Add** icon. In the **Select Network** dialog box, select the network you want to add. To delete an existing network, select the **network** check box, and then click the **Delete** icon.
   • **Extensible Attributes:** Add and delete extensible attributes that are associated with a specific network. You can also modify the values of extensible attributes. For information, see **Using Extensible Attributes**.
   • **Permissions:** This tab appears only if you belong to a superuser admin group. For information, see **Managing Permissions**.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify advanced data.
   • **IPv4 DHCP Options:** Keep the inherited DHCP properties or override them and enter unique settings for the shared network.
     For information, see **Defining IPv4 DHCP Options**.
   • **IPv4 DDNS:** Keep the inherited DDNS settings or override them and enter unique settings for the shared network. Note that you must click **Override** and select **Enable DDN Supdates** for the DDNS settings you configure in this tab to take effect. For information, see **Enabling DDNS for IPv4 and IPv6 DHCP Clients**.
   • **IPv4 BOOTP/PXE:** Keep the inherited BOOTP properties or override them and enter unique settings for the shared network. For information, see **Configuring IPv4 BOOTP and PXE Properties**.
   • **IPv4 Filters:** You can keep the inherited IPv4 logic filters or override them and add a new IPv4 logic filter. For information, see **Applying Filters to DHCP Objects**.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration and click **Restart** if it appears at the top of the screen. or

   Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For
Deleting IPv4 Shared Networks

Though you can delete the networks in a shared network, a shared network must have at least one network in it. To delete a shared network:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Shared Networks section -> shared_network check box, and then select Delete or Schedule Delete from the drop-down menu.
2. To delete the shared network now, in the Delete Confirmation dialog box, click Yes. To schedule the deletion, see Scheduling Deletions.

The appliance puts the deleted shared network in the Recycle Bin, if enabled.

Configuring IPv4 Address Ranges

In a network, you define address ranges from which the DHCP server or failover association assigns IP addresses to client requests. When a DHCP client requests an IP address, the appliance allocates an address within a defined DHCP range. The DHCP client can use the assigned IP address until the lease expires.

When you do not assign a DHCP server or failover association to an address range, the range becomes a reserved range. A reserved range contains IP addresses that are reserved for static hosts, not for dynamic assignments. You can allocate the next available IP from a reserved range.

You can also apply filters to DHCP ranges to control how the DHCP server allocates IP addresses. For information about DHCP filters, see About IPv4 DHCP Filters.

Adding IPv4 Address Ranges

To add an IPv4 address range:

1. Navigate to the IPv4 network to which you want to add an address range, and then select Range from the Add drop down menu.
   or
   From any panel in the DHCP tab, expand the Toolbar and click Add -> Range -> IPv4.
2. In the Add IPv4 Range wizard, select one of the following and click Next:
   - Add Range: Select this to add an address range from scratch.
   or
   - Add Range Using Template: Click Select Template and select the template that you want to use. Note that when you use a template to create an address range, the configurations of the template apply to the new range. The appliance automatically populates the range properties in the wizard. You can then edit the pre-populated properties.
3. Complete the following:
   - Network: Click Select Network. Grid Manager displays the network address here if you have only one network configured. When there are multiple networks, Grid Manager displays the Select Network dialog box from which you can select one.
   - Start: Enter the first available IP address in the range.
   - End: Enter the last available IP address in the range.
   - Name: Optionally, enter a name for the range.
   - Comment: Enter additional information about the address range.
   - Disabled: Select this if you want to save the configuration for the address range but do not want to activate the address range yet. You can clear this check box when you are ready to allocate addresses from this range.

   The Cloud section appears when the Cloud Network Automation license is installed on the Grid Master. For information, see Deploying Cloud Network Automation. To delegate authority for this range, complete the following:

   Delegate authority from the Grid Master

   - Delegate To: This field indicates whether the authority for the range you want to create has already been delegated to a Cloud Platform Appliance. Click Select to choose the Cloud Platform Appliance to which you want to delegate authority. The Member Selector displays only Cloud Platform Appliances in the Grid. Click the member, and Grid Manager displays the member name next to this field. This cloud member now assumes authority for this range, and the Grid Master does not have authority any more. You can also click Clear to remove authority delegation from the selected Cloud Platform Appliance and return authority back to the Grid Master.

4. Click Next and select one of the following:
   - None (Reserved Range): Select this if you want to reserve this address range for static hosts. Addresses in this range cannot be allocated as dynamic addresses. You can allocate the next available IP from this range to a static host. This is selected by default.
   - Grid Member: Select this if you want a Grid member to serve DHCP for this address range. Select a Grid member from the drop-down list. The drop-down list displays only the Grid members that are associated with the network to which the DHCP range belongs.
   - Failover Association: Select this if you want a failover association to serve DHCP for this address range. Click Select Association. In the DHCP Failover Association Selector dialog box, choose a failover association, and then click the Select icon. The appliance lists failover associations that serve DHCP in the network view of the DHCP range. For information, see Chapter 30, DHCP Failover.

5. Click Next to configure or override DHCP options as described in Defining IPv4 DHCP Options.
Note: Steps 6-7 apply only in deployments using Network Insight discovery features. Otherwise, skip to Step 8.

6. Click **Next** to initiate or disable discovery of the new DHCP range.

7. Discovery settings include the following: **Enable Discovery** and **Immediate Discovery**, selecting a Probe member to perform the discovery; and **Polling Options**, which define how the network will be discovered by the Probe member. By default, all Polling Options discovery settings are inherited from the parent network unless you click **Override**. Polling Options govern the protocols used to query and collect information about the network devices being discovered. For more information, see the section **Configuring Discovery Properties** for a complete description of discovery Polling Options.

8. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see **Using Extensible Attributes**.

9. Save the configuration and click **Restart** if it appears at the top of the screen

or

Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Tasks**.

For information on viewing address ranges in a network, see **Viewing IPv4 DHCP Objects**.

**Modifying IPv4 Address Ranges**

You can modify settings for the DHCP range. You can also define an exclusion range to prevent the appliance from assigning the addresses in the exclusion range to clients. IP addresses in an exclusion range are excluded from the pool of IP addresses. For more information, see **About Exclusion Ranges**.

To modify an IPv4 address range:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** section -> **network** -> **addr_range** check box, and then click the Edit icon.
2. The **DHCP Range** editor contains the following basic tabs from which you can modify data:
   - **General**: Modify the fields, except the network address, as described in **Adding IPv4 Address Ranges**.
     When the Cloud Network Automation license is installed on the Grid Master, Grid Manager displays the following information in the **Cloud** section: **Cloud Usage, Owned By**, and **Delegated To**. You cannot modify these fields. For more information, see **Adding IPv4 Address Ranges**.
   - **Member Assignment**: Modify the Grid member or failover association that provides DHCP services for the DHCP range as described in **Adding IPv4 DHCP Options**.
   - **IPv4 DHCP Options**: Keep the inherited DHCP options or override them and enter unique settings for the DHCP range. For information, see **Defining IPv4 DHCP Options**.
   - **Extensible Attributes**: You can add and delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see **Using Extensible Attributes**. You can edit values of inherited extensible attributes by double clicking on the respective column. If an extensible attribute has an inherited value, then the cell is highlighted in blue when you perform an inline editing. The **Descendant Actions** dialog box is displayed when you click **Save**. For information, see **Managing Inheritable Extensible Attributes at the Parent and Descendant Level**. If you delete the value of an inheritable extensible attribute at the parent level, you can choose to preserve the descendant value or remove it. For information, see **Deleting Inheritable Extensible Attributes Associated with Parent Objects**.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see **Managing Permissions**.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify advanced data.
   - **IPv4 DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the DHCP range. Note that you must click **Override** and select **Enable DDNS Updates** for the DDNS settings you configure in this tab to take effect. For information, see **Enabling DDNS for IPv4 and IPv6 DHCP Clients**.
   - **IPv4 BOOTP/PXE**: Keep the inherited BOOTP properties or override them and enter unique settings for the DHCP range. For information, see **Configuring IPv4 BOOTP and PXE Properties**.
   - **Exclusion Ranges**: Configure a range of IP addresses that the appliance does not use to assign to clients. You can use these exclusion addresses as static IP addresses. Enter the start and end addresses of the exclusion range, and optionally, enter information about this exclusion range.
   - **IPv4 DHCP Thresholds**: Keep the inherited thresholds settings or override them and enter unique settings for the DHCP range. For information, see **Configuring Thresholds for DHCP Ranges**.
   - **IPv4 Filters**: You can keep the inherited IPv4 logic filters or override them and add a new IPv4 logic filter. For information, see **Applying Filters to DHCP Objects**.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

or

Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Tasks**.
Controlling Lease Assignments

You can set parameters to control how the DHCP server responds to lease requests within a specific DHCP range. When you set a DHCP range to deny all leases requests, the appliance does not assign IP addresses within this range to DHCP clients. This is useful when you want DHCP clients with IP addresses within this range to obtain new IP addresses when they renew their leases. When a client with an IP address within this range broadcasts a DHCPREQUEST message for its old IP address, the authoritative DHCP server responds with a DHCPNAK. This causes the client to move to the INIT state and to send a DHCPDISCOVER message for a new IP address.

You can also configure the DHCP server to assign or deny IP addresses within a DHCP range to known and unknown DHCP clients. Known clients include roaming hosts and clients with fixed addresses or DHCP host entries. Unknown clients include clients that are not roaming hosts and clients that do not have fixed addresses or DHCP host entries.

To control how the appliance assigns leases to client requests:

1. DHCP Range: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.
2. In the IPv4 Range editor, click Toggle Advanced Mode if the editor is in basic mode. When the additional tabs appear, click the IPv4 DHCP Options tab -> Advanced tab and complete the following:

   **Note:** The IPv4 DHCP Options tab is enabled when you select a Grid Member or IPv4 DHCP Failover Association in the Member Assignments tab.

   - **Allow/Deny Clients**
     - **Known Clients:** Select this check box, and then select **Allow or Deny** from the drop-down list to assign or deny IP addresses within this range to known DHCP clients. Known DHCP clients include roaming hosts and clients with fixed addresses or DHCP host entries. Note that the appliance cannot deny an IP address to a fixed address within this range. You must disable the fixed address if you do not want it to obtain an IP address here.
     - **Unknown Clients:** Select this check box, and then select **Allow or Deny** from the drop-down list to assign or deny IP addresses within this range to unknown DHCP clients. Unknown DHCP clients include clients that are not roaming hosts and clients that do not have fixed addresses or DHCP host entries.

   - **Deny Leases:** Select **Deny all lease requests for this range** to deny all lease requests from DHCP clients.

3. Save the configuration and click Restart if it appears at the top of the screen.

Deleting IPv4 Address Ranges

To delete a DHCP range:

- From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network -> addr_range check box, and then click the Delete icon.

Configuring IPv4 Fixed Addresses

A fixed address represents a persistent link between an IP address and one of the following:

- MAC address
- Client identifier
- Circuit ID or remote ID in the DHCP relay agent option (option 82)

You can create fixed addresses as described in 4823781 or from the Tasks Dashboard. For information about the Tasks Dashboard, see The Tasks Dashboard. You can also create a fixed address when you create a host record or when you convert an active, dynamically leased address to a fixed address. For more information, see Adding Host Records and Converting DHCP Leases.

When you create a fixed address, you must define a host identifier that the DHCP server uses to match the DHCP client. Every time the DHCP client with the matching identifier requests an IP address, the DHCP server assigns it the same address.

When a DHCP client sends a DHCPDISCOVER, it can include the MAC address or a unique client identifier as option 61 in the DHCP section of the packet. Using a client identifier is especially useful for virtualized server processes that might be moved to different hardware platforms. For information about option 61, refer to RFC2132, DHCP Options and BOOTP Vendor Extensions. You can select either the MAC address or client identifier as the host identifier in a fixed address. The DHCP server matches the option 61 value in the client request using either the MAC address or client identifier, depending on your configuration. When a DHCP client renews an IP address using a matching MAC address or client identifier, the DHCP server tracks the allocation of IP addresses and reserves the same IP address for the client.

When you enter a MAC address, you can use one of the following formats:

- aa:bb:cc:dd:ee:ff — Six groups of two hexadecimal digits separated by colons ( :)
- aa-bb-cc-dd-ee-ff — Six groups of two hexadecimal digits separated by hyphens (-)
- aabb:cc:dd:ee:ff — Three groups of four hexadecimal digits separated by colons ( :)
- aabbcc-dd:eeff — Two groups of six hexadecimal digits separated by a hyphen (-)
- aabbccddeeff — One group of 12 hexadecimal digits without any separator

After you save the entry, the appliance displays the MAC address in the AA:BB:CC:DD:EE:FF format.
Adding IPv4 Fixed Addresses

For Cloud Network Automation, you can create IPv4 fixed addresses within the delegation authority of a Cloud Platform Appliance. The newly created fixed address is forwarded to the Cloud Platform Appliance. For information, see About Authority Delegation.

To add an IPv4 fixed address:

1. Navigate to the network to which you want to add a fixed address, and then select Fixed Address from the Add drop-down menu. or
   From any panel in the DHCP tab, expand the Toolbar and click Add -> Fixed Address -> IPv4.
2. In the Add IPv4 Fixed Address wizard, select one of the following and click Next:
   - Add Fixed Address
   - Add Fixed Address using Template

   Click Select Template and select the template that you want to use. Note that when you use a template to create a fixed address, the configurations of the template apply to the new address. The appliance automatically populates the fixed address properties in the wizard. You can then edit the pre-populated properties.

1. Complete the following:
   a. Network: Click Select Network. When there are multiple networks, Grid Manager displays the Select Network dialog box from which you can select one.
   b. IP Address: Enter the IPv4 address for the fixed address, or click Next Available IP to obtain the next available IP address. For information about obtaining the next available IP address, see About the Next Available Network or IP Address. Note that for Cloud Network Automation, Next Available IP is not available if the fixed address you want to create is within a delegated range.
   c. If the network of the IP address is served by a Grid member, Grid Manager displays the AssignIPAddressby section. Select one of the following to match your criteria:
      - MAC Address: Select this to assign a fixed address to a host with the MAC address that you specify here. Enter the MAC address in the field. For MAC address format, see 4823781.
      - DHCP Client Identifier: Select this to assign a fixed address to a host with the DHCP client identifier that you specify here. In the field, enter the client identifier of the host to which you want the DHCP server to assign this IP address. The client identifier must be unique within the network.
      - Match null (\0) at beginning of DHCP client identifier: This is enabled when you select DHCP client identifier. Select this when a DHCP client sends a \000 prefixed to the DHCP client identifier. \0 is the null character. Some DHCP clients (for example, Microsoft) send the client identifier in a \000foo format (with the null character prefix instead of just foo). The client identifier for the requesting host and the client identifier stored in the appliance must match.
      - DHCP Relay Agent: Select this to assign a fixed address to a host with the circuit ID or remote ID you specify here. From the drop-down list, select Circuit ID or Remote ID, and then enter the ID in the field. For information about circuit IDs and remote IDs, see About the DHCP Relay Agent Option (Option 82). You can enter the ID in hexadecimal format, such as ex:aa, ab, 1f:cd, or ef:23:56, or in string format, such as abcd or aa:gg. The appliance matches the value you enter here with the value sent by the DHCP client in counted octet sequence format. For information about how to use hexadecimal values, see DHCP Option Data Types. The ID is case sensitive and can contain up to 230 characters. Regardless of the entry you enter here, you can define the logging format for the circuit ID and remote ID when Grid Manager displays them in the detailed lease information page. For information about how to configure the logging format, see Defining Logging Format for DHCP Option 82.

   d. Name: Enter a name for the Fixed Address. This field is required if the network is served by a Microsoft server. For information, see Adding Fixed Addresses/Microsoft Reservations.
   e. Comment: Optionally, enter additional information about the fixed address.
   f. Disabled: Select this if you do not want the DHCP server to allocate this IP address at this time.

The Cloud section appears when the Cloud Network Automation license is installed on the Grid Master. For information, see Deploying Cloud Network Automation. This section displays the following information:

- Cloud Usage: This field indicates whether this object is associated with any specific cloud extensible attributes or within a scope of delegation. It can be one of the following:
  - Cloud from adapter: Indicates that this object has been created by a cloud adapter and it may or may not be within a scope of delegation at the moment.

---

Note: You cannot use the same circuit ID or remote ID for different fixed addresses if the addresses are in the same network or the same shared network.
• **Cloud from delegation:** Indicates that this object is within the scope of delegation or the object itself defines a scope of authority delegation, and it is not created by a cloud adapter.

• **Used by cloud:** Indicates that this network or network container is associated with the extensible attribute Is External or Is Shared and the value is set to True, which implies the network is a private or shared network managed by the CMP, and it is not Cloud from adapter or Cloud from delegation.

• **Non-cloud:** The object is a regular NIOS object and is not within the scope of any authority delegation nor is it associated with any of these extensible attributes: Cloud API Owned, Is External or Is Shared. NIOS admin users can modify this object based on their permissions.

• **Owned By:** A cloud object can be owned by the Grid Master or the cloud adapter. When the object is created by the Grid Master, this shows Grid. If the object is created by the cloud adapter, this shows Adapter.

**Delegate authority from the Grid Master**

• **Delegate To:** This field indicates whether the authority for the object you want to create has already been delegated. If so, it displays the name of the delegation.

4. (Optional) Click **Next** to configure or override DHCP options as described in About IPv4 DHCP Options on page 1132.

5. (Applies only to Network Insight) **This step is not required for creating a new Fixed Address.** In the following Wizard step, you can optionally define the following identification values and settings for the new object's port reservation:

   • Choose the **Device Type**: Router, Switch-Router, Switch, MSFT (Microsoft) Server, NetMRI, NIOS, VNIO, or ESX (VMware) Server.
     The values on this page are not required for defining the actual port reservation in a later wizard step. Certain device types could be descriptively relevant based on the type of object you are creating. As an example, the MSFT Server designator helps identify the new object as a Microsoft Hyper-V Host. The ESX Server designator can be used to identify the new object as a VMware ESX Host. These values are not required and will not affect the functionality of the object.

   • Choose the **Device Vendor**: Cisco, Juniper, Aruba, Dell, Infoblox, or HP.

   • You can also enter a **Location** and a **Description**. These values are advisory and not required for configuration. After you define this group of settings, you can also define a device port reservation, which is done in a later step. This is not required for the Fixed Address object creation.

6. Click **Next** to initiate or disable discovery of the new Fixed Address. (Applies only to Network Insight) **This step is not required for creating a new Fixed Address.**

   a. Choose either **Exclude from Network Discovery** or **Enable Immediate Discovery.** If you choose to Exclude, discovery will not execute on the fixed IP address. If you choose **Enable Immediate Discovery,** discovery will execute on the object after you save your settings. You may also choose to leave both options disabled.

   b. By default, the new fixed address object inherits its SNMP credentials from those defined at the grid level. Should you wish to override them for a local set of credentials, check the **Override Credentials** check box and select the **SNMPv1/SNMPv2** or **SNMPv3** option and enter the locally used credentials.

   c. You may also test the entered SNMP credentials by clicking **Test SNMP Credential.**

**Note:** For descriptions of SNMP credentials for discovery, see the section **Configuring SNMPv1/v2 Credentials for Polling** and **Configuring SNMPv3 Properties**. These Grid-based values are inherited, by default, by each new object you create.

7. Choose either **Exclude from Network Discovery** or **Enable Immediate Discovery.** If you choose to Exclude, discovery will not execute on the fixed IP address. If you choose **Enable Immediate Discovery,** discovery will execute on the object after you save your settings. You may also choose to leave both options disabled.

   a. By default, the new fixed address object inherits its SNMP credentials from those defined at the grid level. Should you wish to override them for a local set of credentials, check the **Override Credentials** check box and select the **SNMPv1/SNMPv2** or **SNMPv3** option and enter the locally used credentials.

   b. You may also test the entered SNMP credentials by clicking **Test SNMP Credential.**

   c. You can also click **Test CLI Credentials** to enter and test a set of CLI login credentials against a device based on its IP address. Port control operations require CLI credentials for the involved devices. (If you are not using port control for the new object, usage of CLI credentials is optional.) Because some IPAM and DHCP objects will use port control features as part of object creation, CLI credentials are automatically leveraged as part of discovery. Ensure you have the correct sets of CLI credentials for devices in your network. For more information, see the section **Configuring CLI Discovery Properties**.

   d. SSH is the default for CLI operations. Check the **Allow Telnet** check box if you know the device involved in the object assignment may support Telnet but may not support SSH, or if you want Telnet as an option.

   **Note:** All port configuration operations require CLI credentials to be entered into Grid Manager. Because some IPAM and DHCP objects will use port control features as part of object creation, CLI credentials are automatically leveraged as part of discovery. Ensure you have the correct sets of CLI credentials for devices in your network.

7. Click **Next** to define port connectivity for the device port that will be associated with the new object. **This step is not required for creating a new Fixed Address.** This feature set is also termed portcontrol in the NIOS/Grid Manager system. The device whose interface the new Fixed Address will be associated should already be discovered by Network Insight.

   a. After choosing the device, choose the **Interface** with which the port reservation will be bound. The drop-down list shows only interfaces that are most recently found to be available by Grid Manager during the last discovery cycle.

   b. The Wizard page also shows a list of any VLANs that are currently configured in the chosen device (The following VLANs are configured). This Wizard page allows only the assignment of an existing VLAN in the chosen device to the new port reservation.

   c. Check the **Configure Port** check box to define port control settings for the port reservation.

   d. Choose the **Data VLAN** and/or the **Voice VLAN** settings you may need for the port assignment. Depending on the selected device, you may or may not be able to apply VLAN settings.

   e. Set the **Admin Status** to **Up** if you need to activate the port after assignment in the current task.
All port control operations require CLI credentials to be configured. Because some IPAM and DHCP objects will use port control features as part of object creation, CLI credentials are automatically leveraged as part of discovery and definition of port configurations such as Admin Up/Down status. Ensure you have the correct sets of CLI credentials for devices in your network.

- Enter a Description for the port assignment. Infoblox recommends doing so to help other technicians to recognize the port assignment task.

8. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes. When you create a new fixed address whose authority is delegated to a Cloud Platform Appliance, the required cloud extensible attributes and their values are automatically populated.

9. As the final step in the Add Fixed Address wizard, you define when Grid Manager creates the new object by scheduling it. You also schedule when the associated port control task executes (if a port configuration is specified).

- To create the new object and its associated port configuration immediately, select Now. Grid Manager synchronizes the port reservation task to take place at the same time as the activation of the new object.
- You can choose to have Grid Manager execute the port reservation task at the same time as the Fixed Address object creation. To do so, select At same time as Fixed Address.
- You can choose to have Grid Manager execute the port reservation task at a later time by selecting Later. Choose a Selected time by entering or selecting a Start Date (click the calendar icon to choose a calendar date) and a Start Time, and choose a Time Zone.

10. Choose one of the following from the Save&... drop-down button menu:

- Click Save & Close to add the new object and close the wizard (this is the default).
- Click Save & Edit to add the new object and launch the editor.
- Click Save & New to add the new object and launch the wizard again to add another Fixed Address object.

Note: At any step during the wizard, you can click Schedule for Later to schedule the task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks. You cannot schedule this task when you are creating an object that is within a delegated scope.

For information on viewing fixed addresses and other DHCP objects, see Viewing IPv4 DHCP Objects.

Modifying IPv4 Fixed Addresses

To modify the settings of a fixed address:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network -> fixed_address check box, and then click the Edit icon.
2. The Fixed Address editor contains the following tabs from which you can modify settings:

   - General: You can modify the fields, except the network address, as described in 4823781 4823781
   - Device Information: Define general identity/type information for the type of device to which your new object connects. For more information, see Adding IPv4 Reservations.
   - Discovery: Checking the Enable Discovery check box informs NIOS to begin discovering the fixed address after you click Save and Close. You manage discovery polling settings local to the fixed address from this page. For a complete overview of features on this page, see Discovering Devices and its subsections.
   - IPv4 DHCP Options: You can keep the inherited DHCP options or override them and enter unique settings for the fixed address. For information, see Defining IPv4 DHCP Options.
   - IPv4 Discovered Data: Displays the discovered data of the fixed address. For information, see Viewing Discovered Data.
   - Port Reservation: Review and edit any device port reservations that may be defined for the current object, or create a new port reservation and schedule it. For a closer look, see the section Port Control Features in Network Insight, and steps 4-8 in the section 4823781.
   - Extensible Attributes: Add and delete extensible attributes that are associated with a specific network. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes. You can edit values of inheritable extensible attributes by double clicking on the respective column. If an extensible attribute has an inherited value, then the cell is highlighted in blue when you perform an inline editing.
   - Permissions: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions.

3. Optionally, you can click Toggle Advanced Mode to display the following tabs from which you can modify advanced data.

   - IPv4 DDNS: You can keep the inherited DDNS settings or override them and enter unique settings for the fixed address. Note that you must click Override and select Enable DDN Supdates for the DDNS settings you configure in this tab to take effect. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients.
   - IPv4 BOOTP/PXE: You can keep the inherited BOOTP properties or override them and enter unique settings for the fixed address. For information, see Configuring IPv4 BOOTP and PXE Properties.
   - IPv4 Filters: You can keep the inherited IPv4 logic filters or override them and add a new IPv4 logic filter. For information, see Applying Filters to DHCP Objects.

Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration and click Restart if it appears at the top of the screen.
Deleting Fixed Addresses

To delete a fixed address within the DHCP range:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network -> fixed_address check box or check boxes. You cannot delete multiple fixed addresses at the same time if the authority for one of the fixed addresses is delegated to a Cloud Platform Appliance.
2. Select Delete from the Delete drop-down list.
3. In the Delete Confirmation dialog box, do the following:
   - Delete associated leases with the fixed address (selected fixed IP address): When you clear this check box and click Yes, the appliance changes the status of the associated leases from Static to Active. When you select this check box and click Yes, the appliance deletes all the leases associated with the fixed address.

Note: NIOS removes all the static leases associated with a fixed address when you delete a fixed address out of the DHCP range, regardless of the selection of the Delete associated leases with the fixed address (selected fixed IP address) check box in the Delete Confirmation dialog box.

To schedule the fixed address deletion:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network -> fixed_address check box.
2. Select Schedule Delete from the Delete drop-down list.
3. In the Schedule Deletion dialog box, complete the following:
   - Delete Now: Select this to delete the object upon clicking Delete Now.
   - Delete Later: Select this to schedule the deletion at a later date and time. Complete the following:
     - Date: Enter the date in YYYY-MM-DD (year-month-day) format. The appliance displays today's date. You can also click the calendar icon to select a date from the calendar widget.
     - Time: Enter the time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.
     - Time Zone: Select a time zone for the scheduled date and time from the drop-down list. This field displays the time zone of the browser that the admin uses to log in to Grid Manager.
   - Delete associated leases with the fixed address: Select this check box to delete all the leases associated with the fixed address.
4. Click Schedule Deletion.

The appliance performs the deletion at the scheduled date and time, and puts all deleted objects in the Recycle Bin, if enabled. You can restore the objects if necessary.

Configuring IPv4 Reservations

You can create a reservation as a static IP address for future use. A reservation is a pre-provisioned fixed address that is associated with a MAC address of 00:00:00:00:00:00. Since 00:00:00:00:00:00 is not a real MAC address, no client can receive this IP address from the address pool. You can reserve this static IP address and assign it to a client in the future.

To create a reservation, you can do one of the following:

- Add a reservation. For information, see Adding IPv4 Reservations.
- Convert a fixed address or a dynamic address with an active lease to a reservation. For information, see Converting Objects Associated with IP Addresses.
- Define a fixed address with an IP address. For information, see Adding IPv4 Fixed Addresses.

Adding IPv4 Reservations

Note: At any step during the wizard, you can click Schedule for Later to schedule the task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

To create a reservation:

1. Navigate to the network to which you want to add a reservation, and then select IPv4 Reservation from the Add drop down menu.
   or
   From any panel in the DHCP tab, expand the Toolbar and click Add -> IPv4 Reservation.
2. In the Add Reservation wizard, select one of the following and click Next:
   - Add Reservation
   or
   - Add Reservation using Template
3. Complete the following:

- **Network**: The displayed network address can either be the last selected network or the network from which you are adding the DHCP range. If no network address is displayed or if you want to specify a different network, click **Select Network**. When there are multiple networks, Grid Manager displays the **Select Network** dialog box from which you can select one.
- **IP Address**: Enter the IP address that you want to reserve for manual assignment, or click **Next Available IP** to obtain the next available IP address. For information about obtaining the next available IP address, see **Adding IPv4 Fixed Addresses**. Note that for Cloud Network Automation, Next Available IP is not available if the reservation you want to create is within a delegated range.
- **Name**: Optionally, enter a name for the reservation.
- **Comment**: Optionally, enter additional information about the reservation.
- **Disabled**: Select this if you do not want the DHCP server to use this reservation at this time.

The **Cloud** section appears when the Cloud Network Automation license is installed on the Grid Master. For information, see **Deploying Cloud Network Automation**. This section displays the following information:

- **Cloud Usage**: This field indicates whether this object is associated with any specific cloud extensible attributes or within a scope of delegation. It can be one of the following:
  - **Cloud from adapter**: Indicates that this object has been created by a cloud adapter and it may or may not be within a scope of delegation at the moment.
  - **Cloud from delegation**: Indicates that this object is within the scope of delegation or the object itself defines a scope of authority delegation, and it is not created by a cloud adapter.
  - **Used by cloud**: Indicates that this network or network container is associated with the extensible attribute **Is External** or **Is Shared** and the value is set to True, which implies the network is a private or shared network managed by the CMP, and it is not **Cloud from adapter** or **Cloud from delegation**.
  - **Non-cloud**: The object is a regular NIOS object and is not within the scope of any authority delegation nor is it associated with any of these extensible attributes: **Cloud API Owned**, **Is External** or **Is Shared**. NIOS admin users can modify this object based on their permissions.
  - **Owned By**: A cloud object can be owned by the Grid Master or the cloud adapter. When the object is created by the Grid Master, this shows **Grid**. If the object is created by the cloud adapter, this shows **Adapter**.

**Delegate authority from the Grid Master**

- **Delegate To**: This field indicates whether the authority for the object you want to create has already been delegated. If so, it displays the name of the delegation.

4. Click **Next** to configure or override DHCP options as described in **Defining IPv4 DHCP Options**.

5. **(Applies only to Network Insight)** This step is not required for creating a new IPv4 Reservation. In the following Wizard step, you can optionally define the following identification values and settings for the new object's port reservation:

- **Choose the Device Type**: **Router**, **Switch-Router**, **Switch**, **MSFT (Microsoft) Server**, **NetMRI, NIOS, VNIOs**, or **ESX (VMware) Server**.

  The values on this page are not required for defining the actual port reservation in a later wizard step. Certain device types could be descriptively relevant based on the type of object you are creating. As an example, the **MSFT Server** designator helps identify the new object as a Microsoft Hyper-V Host. The **ESX Server** designator can be used to identify the new object as a VMware ESX Host. These values are not required and will not affect the functionality of the object.

- **Choose the Device Vendor**: **Cisco, Juniper, Aruba, Dell, Infoblox**, or **HP**.

  You can also enter a **Location** and a **Description**. These values are advisory and are not required for configuration. After you define this group of settings, you will still need to define a device port reservation, which is done in a later step.

6. **(Applies only to Network Insight)** Click **Next** to initiate or disable discovery of the new IPv4 reservation.

- **Choose either Exclude from Network Discovery** or **Enable Immediate Discovery**. If you choose to Exclude, discovery will not execute on the object. If you choose Enable Immediate Discovery, discovery will execute on the object after you save your settings. You may also choose to leave both options disabled.

  - **By default**, the new object inherits its SNMP credentials from those defined at the grid level. **Should you wish to override them for a local set of credentials, check the Override Credentials check box and select the **SNMPv1/SNMPv2** or **SNMPv3** option and enter the locally used credentials. For more information, see the sections **Configuring SNMPv1/v2 Credentials for Polling** and **Configuring SNMPv3 Properties** for a complete description of SNMP credentials for discovery.

  - **For the new object**, you can check the **Override CLI Credentials** check box to override the inherited set of CLI credentials taken from the Grid level. This set of credentials may be used for the device that is directly associated with the new object (in this case, an IPv4 Reservation) in its port reservation.

  - **You can also click Test CLI Credentials** to select and test a set of CLI login credentials against a device based on its IP address.

  - **Port control tasks require CLI credentials for the involved devices.** (If you are not using port control for the new object, usage of CLI credentials is not required.) Because some IPAM and DHCP objects will use port control features as part of object creation, CLI credentials are automatically leveraged as part of discovery. Ensure you have the correct sets of CLI credentials for devices in your network. For more information, see the section **Configuring CLI Discovery Properties**.

  - **SSH** is the default for CLI operations. Check the **Allow Telnet** check box if you know the device involved in the object assignment may support Telnet but may not support SSH, or if you want Telnet as an option.
7. (Applies only with Network Insight) Click Next to define optional device port association for the IPv4 reservation. This step is optional and not required for creating the new IPv4 Reservation. This feature set is also termed port control in the NIOS/Grid Manager system. The device to which the new object will be associated should already be discovered and managed from the Infoblox Grid.

- Begin by checking the Reserve Port check box. Note that reserving a switch port does not guarantee its availability.
- Optionally, you can skip connecting port configuration by clicking Next.
- Click the Clear button to remove the selected device from the configuration.
- Click the Select Device button to choose the device for which the port reservation will be associated. You should know the identity of the device to whose interface the new object will be associated before taking this step. For more information, see the section Using the Device Selector.
- After choosing the device, choose the Interface with which the reservation will be bound. The drop-down list shows only interfaces that are most recently found to be available by Grid Manager during the last discovery cycle.
- The Wizard page also shows a list of any VLANs that are currently configured in the chosen device (The following VLANs are configured). This Wizard page allows only the assignment of an existing VLAN in the chosen device to the new port reservation.
- Check the Configure Port check box to define specific port configuration settings for the port reservation.
- Choose the DataVLAN and/or the VoiceVLAN settings you may need for the port assignment. Depending on the selected device, you may or may not be able to apply VLAN settings.
- Set the AdminStatus to Up if you need to activate the port after assignment in the current task.
- All port control operations require CLI credentials to be entered into Grid Manager. Because some IPAM and DHCP objects will use port control features as part of object creation, CLI credentials are automatically leveraged as part of discovery and definition of port configurations such as Admin Up/Down status. Ensure you have the correct sets of CLI credentials for devices in your network.
- Enter a Description for the port reservation. Infoblox recommends doing so to help other technicians to recognize the port assignment task.

8. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes.

9. As the final step in the Add IPv4 Reservation wizard, you define when Grid Manager creates the new object by scheduling it. You also schedule when the associated port control task executes (if a port configuration is specified).

- To create the new IPv4 Reservation and its associated port reservation immediately, select Now. Grid Manager synchronizes the port control task to take place at the same time as the activation of the new object.
- You can choose to have Grid Manager execute the port control task at the same time as the object creation. To do so, select At same time as IPv4 Reservation.
- You can choose to have Grid Manager execute the port control task at a later time by selecting Later. Choose a Selected time by entering or selecting a Start Date (click the calendar icon to choose a calendar date) and a Start Time, and choose a Time Zone.

10. Choose one of the following from the Save &... drop-down button menu:

- Click Save & Close to add the new object and close the wizard (this is the default).
- Click Save & Edit to add the new object and launch the editor.
- Click Save & New to add the new object and launch the wizard again to add another IPv4 Reservation object.

11. Click Restart if it appears at the top of the screen.

Note: At any step during the wizard, you can click Schedule for Later to schedule the task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks. You cannot schedule this task when you are creating an object that is within a delegated scope.

Modifying IPv4 Reservations

To modify an IPv4 reservation:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network -> reservation check box, and then click the Edit icon.
2. The Reservation Address editor contains the following tabs from which you can modify data:

   - General: Modify the fields, except the network address, as described in Adding IPv4 Reservations.
   - Device Information: Define general identity/type information for the type of device to which your new object connects. For more information, see Step 5 in the previous section, Adding IPv4 Reservations.
   - IPv4 DHCP Options: Keep the inherited DHCP options or override them and enter unique settings for the reservation. For information, see Defining IPv4 DHCP Options.
   - IPv4 Discovered Data: Displays the discovered data of the reservation. For information, see Viewing Discovered Data.
   - Port Reservation: Review and edit any device port reservations that may be defined for the current object, or create a new port reservation and schedule it. For a closer look, see the section Port Control Features in Network Insight, and steps 4-8 in the section Adding IPv4 Reservations.
   - Extensible Attributes: Add and delete extensible attributes that are associated with a reservation. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes. You can edit values of inheritable extensible attributes by double clicking on the respective column. If an extensible attribute has an inherited value, then the cell is highlighted in blue when you perform an inline editing. The Descendant Actions dialog box is displayed when you click Save. For
information, see Managing Inheritable Extensible Attributes at the Parent and Descendant Level. If you delete the value of an inheritable extensible attribute at the parent level, you can choose to preserve the descendant value or remove it. For information, see Deleting Inheritable Extensible Attributes Associated with Parent Objects.

- **Permissions:** This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify advanced data.

- **IPv4 DDNS:** Keep the inherited DDNS settings or override them and enter unique settings for the reservation. Note that you must click **Override** and select Enable DDN Supdates for the DDNS settings you configure in this tab to take effect. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients.
- **IPv4 BOOTP/PXE:** You can keep the inherited BOOTP properties or override them and enter unique settings for the reservation. For information, see Configuring IPv4 BOOTP and PXE Properties.
- **IPv4 Filters:** You can keep the inherited IPv4 logic filters or override them and add a new IPv4 logic filter. For information, see Applying Filters to DHCP Objects.

Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

**Note:** At any step during the wizard, you can click **Schedule for Later** to schedule the task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks. You cannot schedule this task when you are creating an object that is within a delegated scope.

---

**Viewing IPv4 DHCP Objects**

To view the address ranges, fixed addresses and reservations in a network:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range.
2. Grid Manager displays the following information:
   - **IP Address:** The IP address of the object in the DHCP range. For exclusion ranges, this displays the start and end IP addresses. For host records with multiple IP addresses, each IP address is displayed separately. The appliance highlights disabled DHCP objects in gray. A DHCP object can be a fixed address, reservation, host configured for DHCP, or roaming host with an allocated IP address.
   - **Type:** The object type, such as Fixed Address.
   - **Name:** The object name. For example, if the IP address belongs to a host record, this field displays the hostname.
   - **Fingerprint:** The name of the DHCP fingerprint or vendor ID of the network device that was identified through DHCP fingerprint detection. This field displays No Match for devices that do not have any DHCP fingerprint information. For information about DHCP fingerprints, see DHCP Fingerprint Detection.
   - **Comment:** The information you entered for the object.
   - **Site:** The site to which the object belongs. This is one of the predefined extensible attributes. You can edit values of inheritable extensible attributes by double clicking on the respective column. If an extensible attribute has an inherited value, then the cell is highlighted in blue when you perform an inline editing.

You can select Disabled or available extensible attributes for display.
You can also do the following:

- Sort the data in ascending or descending order by column.
- Create a bookmark for the range.
- Delete or schedule the deletion of a selected object or multiple objects in the range.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Select an object and view detailed information.
- Print or export the data.

---

**About Roaming Hosts**

A roaming host is a host with a dynamically assigned IP address and a specific set of properties and DHCP options. When you create a roaming host for a network device, the device can receive any dynamically assigned address from the network to which it belongs. You can create roaming hosts for devices, such as laptop computers and mobile phones, that require different IP addresses each time they are moved from one network to another and require a unique set of DHCP options.

You can configure IPv4 addresses, IPv6 addresses, or IPv4 and IPv6 addresses for roaming hosts that require both types of addresses. When you configure IPv4 addresses for a roaming host, you must specify the host MAC address or a DHCP client identifier that the appliance uses to match the host, and specify DHCP options for the host. The appliance assigns an IP address from the DHCP range associated with the network from which the address request originates. You can configure an IPv6 prefix or address for a DHCP client. When you do, you must specify the DUID of the host so the appliance can use the DUID to match the host.

A roaming host also receives DHCP options from the Grid, member, network, or shared network with which it associates.

When you configure a roaming host, you must configure it in a specific network view. If you have multiple network views, you must specify the network view to which the requesting hosts belong so the appliance can assign addresses to the hosts from the networks within the same network view.
After you enable support for roaming hosts at the Grid level, you can add a roaming host that supports IPv4, IPv6, or both protocols. You can also convert an IPv4 roaming host to an IPv6 roaming host and vice versa, or convert an IPv4 or IPv6 roaming host to one that supports both IPv4 and IPv6.

**Configuring Roaming Hosts**

To configure a roaming host, perform the following tasks:

1. Enable support for roaming hosts at the Grid level. For information, see 4823788.
2. Add a roaming host.
   - To add an IPv4 roaming host, see 4823788
   - To add an IPv6 roaming host, see 4823788
   - To add a dual stack roaming host, see 4823788

Optionally, configure DHCP properties for the roaming host. You can override properties set for the upper levels and enter unique values for the roaming hosts. For information, see *Defining IPv4 DHCP Options*.

You can do the following after you configure roaming hosts:

- View the configured roaming hosts. For information, see 4823788
- Modify existing roaming hosts. For information, see 4823788
- Delete roaming hosts that are not currently in use. For information, see 4823788

**Enabling Support for Roaming Hosts**

You must first enable support for roaming hosts before adding them. After you enable this feature, you can disable it only after you delete all the existing roaming hosts.

To enable support for roaming hosts:

1. From the *Data Management* tab, select the *DHCP* tab.
2. Expand the Toolbar and click *Grid DHCP Properties*.
3. In the *General Advanced* tab, select *Enable support for roaming host*.
4. Save the configuration and click *Restart* if it appears at the top of the screen.

**Adding IPv4 Roaming Hosts**

To add an IPv4 roaming host:

1. From the *Data Management* tab, select the *DHCP* tab.
2. Select a network view from the drop-down list.
3. Expand the Toolbar and click *Add > Roaming Host > IPv4*.
4. In the *Add Roaming Host* wizard, select one of the following and click *Next*:
   - Add Roaming Host
   - Add Roaming Host using Template
     - Click *Select Template* to create a roaming host using a fixed address/reservation template. In the *DHCP Template Selector* dialog box, select the template that you want to use. Note that when you use a template to create a roaming host, the configurations of the template apply to the new host. The appliance automatically populates the host properties in the wizard. You can then edit the pre-populated properties.

5. Complete the following:
   - **Name**: Enter the name of the roaming host. The name must be unique for each roaming host in a given network view.
   - **Assign IPv4 Address by**: Select one of the following criteria on which the appliance matches when assigning an IP address to the host.
     - **MAC Address**: Select this to assign a dynamic IP address to a host, provided that the MAC address of the requesting host matches the MAC address that you specify here.
     - **DHCP Client Identifier**: Select this to assign a dynamic IP address to a host with the same DHCP client identifier that you specify here. When you select this, the *Match null (0) at beginning of DHCP client identifier* check box is displayed. Select this when a DHCP client sends a `\000` prefix to the DHCP client identifier. `\0` is the null character. Some DHCP clients (for example, Microsoft) send the client identifier in a `\000foo` format (with the null character prefix instead of just `foo`). The client identifier for the requesting host and the client identifier stored in the appliance must match.
   - **Comment**: Enter useful information about the roaming host.
   - **Disabled**: Select this if you do not want the DHCP server to use this roaming host definition. When you disable a roaming host, the host gets an IP address without the defined DHCP options.

6. Click *Next* to configure the IDHCP options for the roaming host, as described in *Defining IPv4 DHCP Options*.

7. Click *Next* to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes*.
8. Save the configuration and click **Restart** if it appears at the top of the screen. **or**
Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Tasks**.

### Adding IPv6 Roaming Hosts

To add an IPv6 roaming host:

1. From the **Data Management** tab, select the **DHCP** tab.
2. Select a network view from the drop-down list.
3. Expand the Toolbar and click **Add -> Roaming Host -> IPv6**.
4. In the **Add Roaming Host** wizard, select one of the following and click **Next**:
   - **Add IPv6 Roaming Host**
   - **Add Roaming Host Using IPv6 Template**

Click **Select IPv6 Template** to create a roaming host using an IPv6 fixed address template. In the **DHCP Template Selector** dialog box, select the template that you want to use. Note that when you use a template to create a roaming host, the configurations of the template apply to the new host. The appliance automatically populates the host properties in the wizard. You can then edit the pre-populated properties.

5. Complete the following:
   - **Name**: Enter the name of the roaming host. The name must be unique for each roaming host in a given network view.
   - **DUID**: Enter the DHCP unique identifier of the host.
   - **Comment**: Optionally, enter additional information about the roaming host.
   - **Disabled**: Select this if you do not want the DHCP server to use this roaming host definition. When you disable a roaming host, the host gets an IP address without the defined DHCP options.

6. Click **Next** to configure the DHCP options for the roaming host, as described in **Defining General IPv6 Properties**.

7. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see **Using Extensible Attributes**.

8. Save the configuration and click **Restart** if it appears at the top of the screen. **or**

Click the Schedule icon at the top of the wizard to schedule this task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Tasks**.

### Adding IPv4/IPv6 Roaming Hosts

To add an IPv4/IPv6 roaming host:

1. From the **Data Management** tab, select the **DHCP** tab.
2. Select a network view from the drop-down list.
3. Expand the Toolbar and click **Add -> Roaming Host -> Both**.
4. In the **Add Roaming Host** wizard, select one of the following and click **Next**:
   - **Add Roaming Host**
   - **Add Roaming Host using Both IPv4 and IPv6 Templates**

   When you use both templates to create a roaming host, the appliance applies the IPv4 template and then the IPv6 template. Therefore, the comments and extensible attributes from the IPv6 template override those from the IPv4 template.

5. Complete the following:
   - **Name**: Enter the name of the roaming host. The name must be unique for each roaming host in a given network view.
   - **Assign IP Address by**: Select one of the following criteria on which the appliance matches when assigning an IP address to the host.
     - **MAC Address**: Select this to assign a dynamic IP address to a host, provided that the MAC address of the requesting host matches the MAC address that you specify here.
     - **DHCP Client Identifier**: Select this to assign a dynamic IP address to a host with the same DHCP client identifier that you specify here. When you select this, the **Match null (\0) at beginning of DHCP client identifier** check box is displayed. Select this when a DHCP client sends a `\000` prefixed to the DHCP client identifier. `\0` is the null character. Some DHCP clients (for example, Microsoft) send the client identifier in a `\000foo` format (with the null character prefix instead of just foo). The client identifier for the requesting host and the client identifier stored in the appliance must match.
   - **DUID**: Specify the DHCP unique identifier of the host.
Viewing Roaming Hosts

To view a list of roaming hosts in a specific network view:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Roaming Hosts.
2. From the Network View drop-down list, select the network view to which the roaming hosts belong.
3. The Grid Manager displays the following for each roaming host:
   - **Name**: The name of the roaming host.
   - **Address**: The IP address of the roaming host.
   - **Comment**: The information that you entered for the roaming host.
   - **Site**: The site to which the template belongs. This is one of the predefined extensible attributes.

You can select **Disabled** and available extensible attributes for display.

You can also do the following:

- Sort the displayed data in ascending or descending order by column.
- Use filters and the **Go** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go** field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.

Setting Properties for Roaming Hosts

You can modify an existing roaming host to add, modify or delete IPv4 or IPv6 addresses, and to set IPv4 and IPv6 DHCP properties.

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Roaming Hosts section -> roaming_host check box, and then click the Edit icon.
2. The RoamingHost editor contains the following tabs from which you can modify data:
   - **General**: Edit the fields as described in 4823788, except for the Templates field.
   - **IPv4 DHCP Options**: Keep the inherited DHCP options or override them and enter unique settings for the roaming host. For information, see Defining IPv4 DHCP Options.
   - **IPv6 DHCP Options**: Keep the inherited IPv6 DHCP properties or override them. For more information, see Defining General IPv6 Properties.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with a roaming host. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify advanced data.

   - **IPv4DNS**: Click **Override** and select **Enable DDNS updates** for the DDNS settings you configure in this tab to take effect. You can specify the following:
     - **DDNS Domain Name**: Specify the domain name that the appliance uses to update DNS.
     - **DDNS Hostname**: Select the Replace the host name dynamically provided by the client/member with the roaming host name check box to use the name of the roaming host record as the name of the client for DDNS updates.

For information about DDNS, see Chapter 21, Configuring DDNS Updates.

   - **IPv4 BOOTP/PXE**: Keep the inherited PXE and BOOTP properties or override them and enter unique settings for the roaming host. For information, see Configuring DHCP for IPv4.
   - **IPv6 DDNS**: Click **Override** and select **Enable DDNS Updates** for the DDNS settings you configure in this tab to take effect.
You can specify the following:

- **DDNS Domain Name**: Specify the domain name that the appliance uses to update DNS.
- **DDNS Hostname**: Select the Replace the host name dynamically provided by the client/member with the roaming host name check box to use the name of the roaming host record as the name of the client for DDNS updates.

For information about DDNS, see Chapter 21, Configuring DDNS Updates.

Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

You can also click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

### Deleting Roaming Hosts

To delete a roaming host:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Roaming Hosts** -> roaming_host check box, and then select **Delete** or **Schedule Delete** from the drop-down menu.

2. To delete the roaming host now, in the **Delete Confirmation** dialog box, click **Yes**. To schedule the deletion, see Scheduling Deletions. The Grid Manager puts the deleted roaming host in the Recycle Bin, if enabled.

### Chapter 28 Managing DHCP Templates

This chapter explains how to configure and manage IPv4 and IPv6 DHCP templates. It contains the following sections:

- 4823792
  - **About IPv4 DHCP Templates**
    - **About IPv4 Range Templates**
    - **About IPv4 Fixed Address/Reservation Templates**
    - **About IPv4 Network Templates**
    - Configuration Example: Creating an IPv4 Network Using a Template
  - **About IPv6 DHCP Templates**
  - **About IPv6 Range Templates**
  - **About IPv6 Fixed Address Templates**
  - **About IPv6 Network Templates**
  - **Viewing Templates**
  - **Deleting Templates**

### About DHCP Templates

A template contains a set of predefined properties that you use to create IPv4 and IPv6 DHCP objects. It is metadata that you can modify and reuse. Using a template enables you to create objects in a quick and consistent way. You can define the object properties once in a template, and then create multiple objects that inherit their properties from the template. For example, you can create a network template that has a fixed netmask of /24 and extensible attribute “State” set to California. You can then use the template to create networks in California that contain /24 netmasks.

You can also modify and delete a template. Note that modifying or deleting a template does not affect existing objects created based on the template. You must be a superuser or have read/write permissions to add, modify, or delete a template. A superuser can set other admin group privileges on templates. For information, see Administrative Permissions for IPv4 or IPv6 DHCP Templates. You can also define extensible attributes for these templates when you create them. For information, see Using Extensible Attributes.

### About IPv4 DHCP Templates

You can use templates to create DHCP IPv4 ranges, fixed addresses, reservations, roaming hosts, and networks. You can create the following IPv4 templates:

- A DHCP range template, containing DHCP range settings, such as the total number of IP addresses allocated to a range. You can add a DHCP range template to a network template. For information, see About IPv4 Range Templates.
- A fixed address/reservation template, containing information for creating fixed addresses, reservations, or roaming hosts. You can add a fixed address/reservation template to a network template. For information, see About IPv4 Network Templates.
- A network template, containing basic network properties for creating networks. It is also a container that holds your DHCP range templates and fixed address/reservation templates. When you create a network using a network template, the network inherits the properties of the range and fixed address/reservation templates. You can create a network in any network view using a network template. For information, see About IPv4 Network Templates.

Because you can potentially add DHCP range and fixed address/reservation templates to a network template, create the DHCP range and fixed address/reservation templates before you create a network template. For information, see Configuration Example: Creating an IPv4 Network Using a Template.
About IPv4 Range Templates

When you create an IPv4 range template, the start and end address fields are based on the specified offset from the network start address and the number of IP addresses in the range. After you create a DHCP range template, you can configure additional properties such as exclusion ranges and DHCP filters, as described in Modifying IPv4 Range Templates. Then when you use the template to create a DHCP range, the range inherits the properties of the template. You can also include a DHCP range template in a network template to automatically create a DHCP range when you use that network template.

If you have deployed the Cloud Network Automation license on the Grid Master, you can configure range templates for cloud delegation. When you select a default Cloud Platform Appliance for a template, all ranges you create using this template will delegate authority to the same Cloud member. Note that when a Cloud member is removed from the Grid, the delegation will also be removed from the template. For information about Cloud Network Automation, see Deploying Cloud Network Automation.

Adding IPv4 Range Templates

To create an IPv4 DHCP range template:

1. From the Data Management tab, select the DHCP tab -> Templates tab, and then expand the Toolbar and click Add -> Templates -> Range -> IPv4.
2. In the Add IPv4 Range Template wizard, do the following:
   - **Name:** Enter a name that helps identify the DHCP range template. For example, enter Region 1 IT if you want to use this template to create DHCP ranges for the IT department in Region 1.
   - **Offset:** An offset in a DHCP range template determines the starting IP address of the range. The appliance adds the offset value you enter here to the start IP address of the network in which you create a DHCP range using this template. That IP address becomes the start IP address of the DHCP range. For example, if you specify an offset value of 25 for a 25.0.0.0/8 network using the DHCP range template, the appliance creates a DHCP range with the start IP address of 25.0.0.25 in the network.
   - **Number of Addresses:** Enter the total number of IP addresses to be included in the DHCP range.
   - **Comment:** Enter useful information about the template.

The Cloud section appears when the Cloud Network Automation license is installed on the Grid Master. For information, see Deploying Cloud Network Automation. To configure this template for cloud delegation, complete the following:

**Use for cloud delegation:** Select this check box to enable cloud delegation for this template.

**Delegate authority from the Grid Master**

- **Delegate To:** In a non-cloud API request, this parameter defines the default member to which authority is delegated. In a cloud API request, the appliance ignores this parameter, which allows you to use this template to create an object on different Cloud Platform Appliances. Click Select to choose the default Cloud Platform Appliance to which you want to delegate authority. The Member Selector displays only Cloud Platform Appliances in the Grid. Click the member, and Grid Manager displays the member name next to this field.

3. Click Next and select one of the following to provide DHCP services for the range:

   - **None (Reserved Range):** Select this if you want to reserve this address range for static hosts. Addresses in this range cannot be allocated as dynamic addresses. You can allocate the next available IP from this range to a static host. This is selected by default.
   - **Grid Member:** Click Select and choose a Grid member from the drop-down list.
   - **Failover Association:** Click Select and choose a failover association. Only failover associations that provide DHCP services in the network view of the DHCP range appear in the drop-down list.
   - **Microsoft DHCP Server:** Click Select and choose a Microsoft server from the drop-down list. The drop-down list displays only the servers that are associated with the network to which the DHCP range belongs.

4. Click Next to configure or override DHCP options as described in Defining IPv4 DHCP Options.

5. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes.

6. Save the configuration and click Restart if it appears at the top of the screen.

Modifying IPv4 Range Templates

After you use the wizard to create an IPv4 DHCP range template, you can set additional properties for the template. Following are some guidelines:

- In the DHCP Options tab of a DHCP range template, the broadcast address is an address offset number rather than a broadcast IP address; network router addresses are offset numbers as well.

An offset in a DHCP range template indicates the starting IP address of the DHCP range object created from the template. For example, you can create a network template called test_network_template and a DHCP range template test_range_template linked to this network template. If the test_range_template has an offset value 10, when you create a 10.0.0.0/8 network using the test_network_template, the appliance creates a DHCP range with the starting IP address 10.0.0.10. If you create a 20.0.0.0/8 network using the test_network_template, the appliance creates a DHCP range with the starting IP address 20.0.0.10.
For the exclusion range in the template, the start and end addresses are determined by the number of offsets in the DHCP range template's start address and the number of IP addresses in the exclusion range. For more information about exclusion ranges, see About DHCP Ranges.

To modify and set properties for a DHCP range template:

1. From the Data Management tab, select the DHCP tab -> Templates tab -> template check box, and then click the Edit icon.
2. The DHCP Range Template editor contains the following tabs from which you can modify data:
   - General: Modify general information described in Adding IPv4 Range Templates.
   - Member Assignment: Change the Grid member, failover association, or Microsoft server that provides DHCP services for this template. You can also add or delete a member or failover association. For information, see Adding IPv4 Address Ranges.
   - IPv4 DHCP Options: Keep the inherited DHCP options or override them and enter unique settings for the template. For information, see Defining IPv4 DHCP Options.
   - Extensible Attributes: Add and delete extensible attributes that are associated with this template. You can also modify the values of the extensible attributes. For information, see Using Extensible Attributes.
   - Permissions: This tab appears only if you belong to a superuser admin group. For information, see About Administrative Permissions.

3. Optionally, you can click Toggle Advanced Mode to display the following tabs from which you can modify data:
   - IPv4DDNS: Keep the inherited DDNS settings or override them and enter unique settings for the template. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients.
   - IPv4 BOOTP/PXE: Keep the inherited BOOTP properties or override them and enter unique settings for the template. For information, see Configuring IPv4 BOOTP and PXE Properties.
   - Exclusion Ranges: Configure a range of IP addresses that the appliance does not use for dynamic address assignments. Complete the following:
     - Offset: An offset for an exclusion range determines the start IP address of the exclusion range. The appliance adds the offset value you enter here to the start IP address of the DHCP range created using this template. That IP address becomes the start IP address of the exclusion range.
     - Number of Addresses: Enter the number of IP addresses to be included in the exclusion range.
     - Comment: Enter useful information about the exclusion range.
   - IPv4 DHCP Thresholds: Keep the inherited thresholds settings or override them and enter unique settings for the template. For information, see Configuring Thresholds for DHCP Ranges.

4. Save the configuration and click Restart if it appears at the top of the screen.

**Note:** Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

### About IPv4 Fixed Address/Reservation Templates

You can use an IPv4 fixed address/reservation template to create fixed addresses, reservations and roaming hosts. When you create an IPv4 fixed address/reservation template, you can specify an offset and number of addresses. This is used when you include the template in a network template. When you include a fixed address/reservation template in a network template, the DHCP server automatically creates reservations based on the offset and number of addresses you specified in the fixed/address reservation template. It does not create fixed addresses.

After you create a fixed address/reservation template using the wizard, you can configure additional properties as described in Modifying IPv4 Fixed Address/Reservation Templates. Then when you use the template to create a fixed address, it inherits the properties of the template.

If you have deployed the Cloud Network Automation license on the Grid Master, you can configure fixed address templates for cloud delegation. When you configure a template for cloud delegation, all fixed addresses you create using this template will inherit authority delegations from their parent objects. For information about Cloud Network Automation, see Deploying Cloud Network Automation.

### Adding IPv4 Fixed Address/Reservation Templates

To create an IPv4 fixed address/reservation template:

1. From the Data Management tab, select the DHCP tab -> Templates section.
2. Click the Add drop-down list and select IPv4 Fixed Address/Reservation Template.
3. In the Add IPv4 Fixed Address/Reservation Template wizard, enter the following:
   - Name: Enter a name that helps identify the fixed address/reservation template. For example, you can enter HP Printer when you create a template that contains settings for assigning fixed addresses or reservations to HP printers.
   - Comment: Optionally, enter additional information about the template.
   - Use for cloud delegation: When you select this check box, all fixed addresses you create using this template inherit authority delegation from their parent objects.

In the Optional Settings For Range of Objects section, do the following:

- Offset: An offset in a fixed address/reservation template determines the start IP address of the object created from the template. The appliance adds the offset value you enter here to the start IP address of the network in which you create objects using this template. That IP address becomes the start IP address of the object.
- Number of Addresses: Enter the number of IP addresses to be used as fixed addresses, reservations, or roaming hosts.
Note: The appliance uses the offset and number of addresses only when this template is used in a network template.

4. Click Next to configure or override DHCP options as described in Defining IPv4 DHCP Options.

5. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes.

6. Save the configuration and click Restart if it appears at the top of the screen.

Modifying IPv4 Fixed Address/Reservation Templates

To modify a fixed address/reservation template:

1. From the Data Management tab, select the DHCP tab -> Templates tab -> template check box, and then click the Edit icon.
2. The Fixed Address/Reservation Template editor contains the following tabs from which you can modify data:
   - General: Modify general information for the template as described in Adding IPv4 Fixed Address/Reservation Templates.
   - IPv4 DHCP Options: Keep the inherited DHCP options or override them and enter unique settings for the template. For information, see Defining IPv4 DHCP Options.
   - Extensible Attributes: Add and delete extensible attributes that are associated with the template. You can also modify the values of the extensible attributes. For information, see Using Extensible Attributes.
   - Permissions: This tab appears only if you belong to a superuser admin group. For information, see About Administrative Permissions.

3. Optionally, you can click Toggle Advanced Mode to display the following tabs from which you can modify data:
   - IPv4 DDNS: Keep the inherited DDNS settings or override them and enter unique settings for the template. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients.
   - IPv4 Filters: You can keep the inherited IPv4 logic filters or override them and add a new IPv4 logic filter for the template. For information, see Applying Filters to DHCP Objects.
   - IPv4 BOOTP/PXE: Keep the inherited BOOTP properties or override them and enter unique settings for the template. For information, see Configuring IPv4 BOOTP and PXE Properties.

Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration and click Restart if it appears at the top of the screen.

About IPv4 Network Templates

You can create IPv4 network templates to facilitate network configuration. You can use network templates to create networks in any network view. When you create a network template, you do not specify a network address. You enter the network address when you create an actual network from the template. You can specify a netmask or allow the user to define the netmask when they create the actual network.

A network template is useful for setting up a network with fixed addresses and DHCP ranges already defined. You can add DHCP range or fixed address/reservation templates to a network template. Once the fixed address and DHCP range information is set up, the network template contains a range template list and a fixed address/reservation template list.

When you enable support for RIR updates, you can create IPv4 network templates specific for RIR associated networks. For information about RIR updates, see RIR Registration Updates.

If you have deployed the Cloud Network Automation on the Grid Master, you can configure network templates for cloud delegation. When you select a default Cloud Platform Appliance for a template, all networks you create using this template will delegate authority to the same Cloud member. If you want to associate any range or fixed address templates with a network template, ensure that you enable "User for cloud delegation" for the network, range, and fixed address templates. Note that when a Cloud member is removed from the Grid, the delegation will also be removed from the template. For information about Cloud Network Automation, see Deploying Cloud Network Automation.

Adding IPv4 Network Templates

To create a network template:

1. From the Data Management tab, select the DHCP tab -> Templates section.
2. Click the Add drop-down list and select IPv4 Network Template.
3. In the Add IPv4 Network Template wizard, do the following:
   - Regional Internet Registry: This section appears only when support for RIR updates is enabled. For information about RIR, see RIR Registration Updates. Complete the following to create a network template for an RIR IPv4 network container or network:
     - Internet Registry: Select the RIR from the drop-down list. The default is RIPE. When you select None, the network is not associated with an RIR organization.
     - Organization ID: Click Select Organization and select an organization from the RIROrganizationSelector dialog box.
     - Registration Status: The default is Not Registered. When using this template to add an RIR allocated network, you can change this to Registered and select the Do not update registrations check box below. Note that when you select API as the communication method, the registration status will be updated automatically after the registration update is completed. However, when you select Email as the communication method, the registration status will not be
automatically updated. If you are creating a new network and the registration update is completed successfully, the status will be changed to Registered. If the update fails, the status will be changed to Not Registered.

- **Registration Action**: Select the registration action from the drop-down list. When you select Create, the appliance creates the IPv4 network and assigns it to the selected organization. When you select None, the appliance does not send registration updates to RIPE. When you use this template to add an existing RIR allocated network to NIOS, select None. When you use this template to add networks to an RIR allocated network (a parent network), select Create. Ensure that the parent network associated with an RIR organization already exists.

- **Do not update registrations**: Select this check box if you do not want the appliance to submit RIR updates to RIPE. By default, the appliance sends updates to the RIR database based on the configured communication method.

- **Name**: Enter a name that helps identify the network template. For example, you can enter Class C if you want to configure the template for creating Class C networks.

- **Netmask**: Select one of the following options:
  - **Fixed**: Select this and adjust the netmask slider to a fixed netmask for this network template. When you select this option, users cannot specify another netmask when they use this template to create a network. For example, if you select /24 as the fixed netmask, all networks created using this template have a /24 netmask.
  - **Allow User to Specify Netmask**: Select this to allow users to specify the subnet mask when creating networks using this template.

- **Comment**: Optionally, enter additional information about the template.

- **Automatically Create Reverse-Mapping Zone**: This function is enabled if the fixed netmask of the template equals /8, /16, and /24, or if you select the Allow User to Specify Netmask option. Select this if you want the appliance to automatically create the corresponding reverse-mapping zone for the networks created using this template. A reverse-mapping zone is an area of network space for which one or more name servers have the responsibility for responding to address-to-name queries. These zones are created in the DNS view assigned to receive dynamic DNS updates at the network level.

The Cloud section appears when the Cloud Network Automation license is installed on the Grid Master. For information, see Deploying Cloud Network Automation. To configure this template for cloud delegation, complete the following:

**Use for cloud delegation**: Select this check box to enable cloud delegation for this template.

**Delegate authority from the Grid Master**

- **Delegate To**: In a non-cloud API request, this parameter defines the default member to which authority is delegated. In a cloud API request, the appliance ignores this parameter, which allows you to use this template to create an object on different Cloud Platform Appliances. Click Select to choose the default Cloud Platform Appliance to which you want to delegate authority. The Member Selector displays only Cloud Platform Appliances in the Grid. Click the member, and Grid Manager displays the member name next to this field.

4. Click Next and do the following to assign either Grid members or Microsoft DHCP servers to this network template. Ensure that you include members or Microsoft servers that are associated with other templates that you plan to add to this network template. You can assign one or multiple members to this template. However, you cannot assign a combination of NIOS Grid members and vNIOS Grid members to the template. You can also assign multiple Microsoft servers to a template, but you cannot assign a mix of Microsoft servers and Grid members to a template.

- **Add** Infoblox Member: Select this option to add a Grid member as a DHCP server for the networks created using this template. Select the Grid member from the Member Selector dialog box. Keep in mind, DHCP properties for the network are inherited from this member. Networks created using this template can be served by multiple members, but a member can serve networks in one network view only.

- **Add Microsoft Server**: Select this option to add a Microsoft server as a DHCP server for the networks created using this template. Select the Microsoft server from the Microsoft Server Selector dialog box.

5. Click Next to associate Active Directory Sites with the network. For more information, see Associating Active Directory Sites with Networks.

6. Click Next and do the following to include IPv4 address range and fixed address/reservation templates in the network template. Note that when you select a fixed address/reservation template, only reservations, not fixed addresses, are created for networks created using this template. You cannot add a fixed address/reservation template that does not contain an offset value or a total number of IP addresses for a range.

   a. Click the Add icon.

   b. In the DHCP Template Selector dialog box, choose the template that you want to include in this network template. You can choose a DHCP range or fixed address/reservation template. Use SHIFT-click and CTRL-click to select multiple templates.

   c. Click the Select icon.

You can delete a template from the table by selecting it and clicking the Delete icon.

7. Click Next to configure or override DHCP options as described in Defining IPv4 DHCP Options.

8. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes.
If you are adding an RIR network, the RIR network attribute table appears. For information about these attributes and how to enter them, see RIR Network Attributes.

9. Save the configuration and click Restart if it appears at the top of the screen.

Modifying IPv4 Network Templates

To modify a network template:

1. From the Data Management tab, select the DHCP tab -> Templates tab -> template check box, and then click the Edit icon.
2. The IPv4 Network Template editor contains the following tabs from which you can modify data:
   - **General**: Modify general information described in Adding IPv4 Network Templates.
   - **Member Assignment**: Change the Microsoft servers or Grid members that provide DHCP services for this template. For information, see Adding IPv4 Networks.
   - **Templates**: Add or delete DHCP range and fixed address/reservation templates. For information, see About IPv4 Range Templates and About IPv4 Fixed Address/Reservation Templates.
   - **IPv4 DHCP Options**: Keep the inherited DHCP options or override them and enter unique settings for the template. For information, see Defining IPv4 DHCP Options.
   - **RIR Registration**: Modify RIR network information. This tab appears only when support for RIR updates is enabled. For information, see Modifying RIR Network Data.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with the template. You can also modify the values of the extensible attributes. For information, see Using Extensible Attributes.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify data:
   - **IPv4 DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the template. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients.
   - **IPv4 BOOTP/PXE**: Keep the inherited BOOTP properties or override them and enter unique settings for the template. For information, see Configuring IPv4 BOOTP and PXE Properties.
   - **IPv4 Filters**: You can keep the inherited IPv4 logic filters or override them and add a new IPv4 logic filter for the template. For information, see Applying Filters to DHCP Objects.
   - **IPv4 DHCP Thresholds**: Keep the inherited thresholds settings or override them and enter unique settings for the template. For information, see Configuring Thresholds for DHCP Ranges.

Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration and click Restart if it appears at the top of the screen.

Configuration Example: Creating an IPv4 Network Using a Template

This example describes how to create a /24 network template and how to use the template to create a 192.168.2/24 network with the following configurations:

- First address 192.168.2.1 is reserved for the router
- Next 10 addresses (192.168.2.2 to 192.168.2.11) reserved for servers
- Next 10 addresses (192.168.2.12 to 192.168.2.21) reserved for printers
- Next 10 addresses (192.168.2.22 to 192.168.2.31) assigned as fixed addresses
- 100 addresses (192.168.2.32 to 192.168.2.131) reserved for workstations. The appliance assigns these dynamically.
- 10 addresses (192.168.2.42 to 192.168.2.51) are in an exclusion range. If you assigned static addresses to certain hosts in the middle of an address range template, you can exclude the addresses from the address range template so the appliance does not assign these IP addresses to clients

Figure 28.1 illustrates the configurations of the 192.168.2/24 network using the network template you create:

Figure 28.1 Creating a Network Using a Template
Use the following steps to create the sample network template (shown in Figure 28.1).

1. Create the following DHCP range templates. For information, see Adding IPv4 Range Templates.
   - Server template with the following values:
     - **Name:** Servers
     - **Offset:** 2
     - **Number of Addresses:** 10
     - **Comment:** Address range 2 to 11 for Servers
   - Printer template with the following values:
     - **Name:** Printers
     - **Offset:** 12
     - **Number of Addresses:** 10
     - **Comment:** Address range 12 to 21 for printers.
   - Workstation template with the following values:
     - **Name:** Workstations
     - **Offset:** 32
     - **Number of Addresses:** 100
     - **Comment:** Address range 32 to 131 for DHCP on workstations
     - Exclusion range with the following values. You must modify the Workstations template to add the exclusion range. For information, see Modifying IPv4 Range Templates.
       - **Name:** Exclusion
       - **Offset:** 42
       - **Number of Addresses:** 10
       - **Comment:** Excluding addresses 42 to 51 from the DHCP range 32 to 131.

2. Create a fixed address/reservation template with the following values. For information, see Adding IPv4 Fixed Address/Reservation Templates.
   - **Name:** Router
   - **Comment:** Fixed address template
   - **Offset:** 1
   - **Number of Addresses:** 1

3. Create a fixed address/reservation template with the following values. For information, see Adding IPv4 Fixed Address/Reservation Templates.
   - **Name:** myFixedAddress
   - **Comment:** Fixed address template
   - **Offset:** 22
   - **Number of Addresses:** 10

4. Create a network template with the following values. For information, see Adding IPv4 Network Templates.
   - **Name:** myNetworkTemplate
   - **Netmask:** Select /24 as the fixed subnet mask for the network
   - **Comment:** Network template for /24 network
   - **Automatically create are verse-mapping zone:** Select this so that the NIOS appliance automatically creates the corresponding reverse-mapping zone for the network.

5. Add the DHCP range templates Servers, Printers, and Workstations to the network template.
6. Add the fixed address/reservation template $myFixedAddress$ to the network template.

7. Add a fixed address with the following values:

8. Create a network using the network template $myNetworkTemplate$ with the following values. For information, see Adding IPv4 Networks.
   - Address: Enter the IP address 192.168.2.0 of the network that you want to create using the template.
   - Select template: Select the network template $myNetworkTemplate$.

9. To verify your configuration, from the Data Management tab, select the DHCP tab -> Templates tab. Select $myNetworkTemplate$ and click the Edit icon. In the Network Template editor, click the Templates tab. The Grid Manager displays the DHCP range templates and fixed address templates.

10. Click Restart to restart services.

About IPv6 DHCP Templates

You can use templates to create DHCP IPv6 ranges, fixed addresses, roaming hosts, and networks. You can create the following IPv6 templates:

- A DHCP range template that specifies an offset and the total number of addresses in a range. You can add a DHCP range template to a network template. For more information, see About IPv6 Range Templates.
- A fixed address template, containing information for creating fixed addresses and roaming hosts. You can add a fixed address template to a network template. For information, see About IPv6 Fixed Address Templates.
- A network template, containing basic network properties for creating networks. It is also a container that holds your DHCP range templates and fixed address/reservation templates. When you create a network using a network template, the network inherits the properties of the range and fixed address/reservation templates. You can create a network in any network view using a network template. For information, see Adding IPv6 Network Templates.

Because you can potentially add DHCP range and fixed address/reservation templates to a network template, create the DHCP range and fixed address/reservation templates before you create a network template.

About IPv6 Range Templates

You can create range templates to specify an offset and the number of addresses allocated to a range. Note that you cannot create templates for prefix-delegated ranges because the start or end prefix can be outside of the subnet address boundary.

After you create a DHCP range template, you can configure additional properties such as exclusion ranges and DHCP properties, as described in 4823807. Then when you use the template to create a DHCP range, the range inherits the properties of the template. You can also include a DHCP range template in a network template to automatically create a DHCP range when you use that network template.

If you have deployed the Cloud Network Automation license on the Grid Master, you can configure range templates for cloud delegation. If you select a default Cloud Platform Appliance for a template, all ranges you create using this template will delegate authority to the same Cloud member. Note that when a Cloud member is removed from the Grid, the delegation will also be removed from the template. For information about Cloud Network Automation, see Deploying Cloud Network Automation.

Note: Infoblox does not support global IPv6 prefix delegation for IPv6 range templates.

Adding IPv6 Range Templates

To create an IPv6 range template:

1. From the Data Management tab, select the DHCP tab -> Templates tab.
2. Click the Add drop-down menu and select IPv6 DHCP Range Template.
3. In the Add IPv6 Range Template wizard, complete the following:
   - Name: Enter a name that helps identify the IPv6 DHCP range template.
   - Offset: An offset in a DHCP range template determines the starting IP address of the range. The appliance adds the offset value you enter here to the start IP address of the network in which you create a DHCP range using this template. That IP address becomes the start IP address of the DHCP range. For example, you specify an offset value of 10 for the 2001:db8:1263:/48 network using the DHCP range template, the appliance creates a range with the start address 2001:db8:1263:0:0:0:0:a.
   - Number of Addresses: Enter the total number of IPv6 addresses to be included in the DHCP range.
   - Comment: Optionally, enter additional information about the template.

The Cloud section appears when the Cloud Network Automation license is installed on the Grid Master. For information, see Deploying Cloud Network Automation. To configure this template for cloud delegation, complete the following:

Use for cloud delegation: Select this check box to enable cloud delegation for this template.

Delegate authority from the Grid Master

- Delegate To: In a non-cloud API request, this parameter defines the default member to which authority is delegated. In a cloud API request, the appliance ignores this parameter, which allows you to use this template to create an object on different Cloud
Adding IPv6 Fixed Address Templates

To create an IPv6 fixed address template:
1. From the Data Management tab, select the DHCP tab -> Templates tab.
2. Click the Add drop-down menu and select IPv6 Fixed Address Template.
3. In the Add IPv6 Fixed Address Template wizard, enter the following:
   - Name: Enter a name that helps identify the IPv6 fixed address template. For example, you can enter HP Printer when you create a template that contains settings for assigning fixed addresses or reservations to HP printers.
   - Comment: Optionally, enter additional information about the template.
   - Use for cloud delegation: When you select this check box, all fixed addresses you create using this template inherit authority delegation from their parent objects.

Modifying IPv6 Range Templates

You can modify the properties of a DHCP range template and define an exclusion range. For the exclusion range in the template, the start and end addresses are determined by the number of offsets in the DHCP range template's start address and the number of IP addresses in the exclusion range. For more information about exclusion ranges, see About DHCP Ranges.

To modify a DHCP range:
1. From the Data Management tab, select the DHCP tab -> Templates tab -> template check box, and then click the Edit icon.
2. The IPv6 DHCP Range Template editor contains the following tabs from which you can modify data:
   - General: Modify general information as described in 4823807.
   - Member Assignment: Change the Grid member that provides DHCP services for ranges created from this template. For information, see 4823807.
   - Extensible Attributes: Add and delete extensible attributes that are associated with this template. You can also modify the values of the extensible attributes. For information, see Using Extensible Attributes.
   - Permissions: This tab appears only if you belong to a superuser admin group. For information, see About Administrative Permissions.
3. Optionally, you can click Toggle Advanced Mode to display the following tabs from which you can modify data:
   - Exclusion Ranges: Configure a range of IP addresses that the appliance does not use for dynamic address assignments. Exclusion Ranges:
     - Offset: An offset for an exclusion range determines the start IP address of the exclusion range. The appliance adds the offset value you enter here to the start IP address of the DHCP range created using this template. That IP address becomes the start IP address of the exclusion range.
     - Number of Addresses: Enter the number of IP addresses to be included in the exclusion range.
   - Comment: Enter useful information about the exclusion range.

Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration.

About IPv6 Fixed Address Templates

A fixed address template is useful when you want to create multiple fixed addresses in a network. When you create a fixed address template, you specify the offset value and number of fixed addresses to be created. You can also specify additional properties for the fixed addresses. Note that you can use the template to create address-based fixed addresses. You cannot specify prefixes in the template because a fixed address could use a prefix that is not part of the subnet to which the fixed address belongs. You can enter prefixes when you create the individual fixed address objects using the template.

If you have deployed the Cloud Network Automation license on the Grid Master, you can configure fixed address templates for cloud delegation. When you configure a template for cloud delegation, all fixed addresses you create using this template will inherit authority delegations from their parent objects. For information about Cloud Network Automation, see Deploying Cloud Network Automation.
In the **Optional Settings For Range of Objects** section, do the following:

- **Offset**: An offset in a fixed address template determines the IP address of the first fixed address created from the template. The appliance adds the offset value you enter here to the start IP address of the network in which you create objects using this template, and that IP address becomes the IP address of the object. For example, you specify an offset value of 50 for the 2001:db8:1263:48 network, when you create a fixed address using the fixed address template, the appliance assigns it the address 2001:db8:1263:0:0:0:0:32.

- **Number of Addresses**: Enter the number of IP addresses to be used as fixed addresses or roaming hosts.

**Note**: The appliance uses the offset and number of addresses only when this template is used in a network template.

4. Click **Next** to configure or override DHCP options as described in Configuring DHCP Properties.

5. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes.

6. Save the configuration.

### Modifying IPv6 Fixed Address Templates

To modify a fixed address template:

1. From the **Data Management** tab, select the **DHCP** tab -> **Templates** tab -> template check box, and then click the **Edit** icon.

2. The **IPv6 Fixed Address Template** editor contains the following tabs from which you can modify data:
   - **General**: Modify general information for the template as described in Adding IPv6 Fixed Address Templates.
   - **IPv6 DHCP Options**: Keep the inherited DHCP options or override them and enter unique settings for the template. For information, see Defining General IPv6 Properties.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with the template. You can also modify the values of the extensible attributes. For information, see Using Extensible Attributes.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see About Administrative Permissions.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify data:
   - **IPv6 DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the template. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients.

**Note**: Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration.

### About IPv6 Network Templates

You can create IPv6 network templates to facilitate network configuration. You can use network templates to create networks in any network view. When you create a network template, you do not specify a network address. You enter the network address when you create an actual network from the template. You can specify a netmask or allow the user to define the netmask when they create the actual network.

A network template is useful for setting up a network with fixed addresses and DHCP ranges already defined. You can add DHCP range or fixed address templates to a network template.

**Note**: You cannot configure the following DHCP options in an IPv6 network template: server-id (Option 2), preference (option 7), and unicast (Option 12). These options are valid only for a DHCP member.

When you enable support for RIR updates, you can create IPv6 network templates specific for RIR associated networks. For information about RIR updates, see RIR Registration Updates.

You can also configure network templates for cloud delegation if you have deployed the Cloud Network Automation on the Grid Master. If you select a default Cloud Platform Appliance for a template, all networks you create using this template will delegate authority to the same Cloud member. Note that when a Cloud member is removed from the Grid, the delegation will also be removed from the template. For information about Cloud Network Automation, see Deploying Cloud Network Automation.

### Adding IPv6 Network Templates

To create a network template:

1. From the **Data Management** tab, select the **DHCP** tab -> **Templates** tab.

2. Click the Add drop-down menu and select **IPv6 Network Template**.

3. In the Add IPv6 Network Template wizard, do the following:
   - **RegionalInternetRegistry**: This section appears only when support for RIR updates is enabled. For information about RIR, see
RIR Registration Updates. Complete the following to create a network template for an RIR IPv6 network container or network:

- **Internet Registry**: Select the RIR from the drop-down list. The default is RIPE. When you select **None**, the network is not associated with an RIR organization.
- **Organization ID**: Click **Select Organization** and select an organization from the **RIR Organization Selector** dialog box.
- **Registration Status**: The default is **Not Registered**. When using this template to add an RIR allocated network, you can change this to **Registered** and select the **Do not update registrations** check box below. Note that when you select API as the communication method, the registration status will be updated automatically after the registration update is completed. However, when you select **Email** as the communication method, the registration status will not be automatically updated. If you are creating a new network and the registration update is completed successfully, the status will be changed to **Registered**. If the update fails, the status will be changed to **Not Registered**.
- **Registration Action**: Select the registration action from the drop-down list. When you select **Create**, the appliance creates the IPv4 network and assigns it to the selected organization. When you select **None**, the appliance does not send registration updates to RIPE. When you use this template to add an existing RIR allocated network to NIOS, select **None**. When you use this template to add networks to an RIR allocated network (a parent network), select **Create**. Ensure that the parent network associated with an RIR organization already exists.
- **Do not update registrations**: Select this check box if you do not want the appliance to submit RIR updates to RIPE. By default, the appliance sends updates to the RIR database based on the configured communication method.
- **IPv6 Prefix**: If you are adding a template for a previously defined global IPv6 prefix, you can select it from the drop-down list.
- **Name**: Enter a name that helps identify the network template.
- **Netmask**: Select one of the following options:
  - **Fixed**: Select this and adjust the netmask slider to a fixed netmask for this network template. When you select this option, users cannot specify another netmask when they use this template to create a network. For example, if you select /24 as the fixed netmask, all networks created using this template have a /24 netmask. The slider moves to the CIDR value associated with the selected prefix when you choose a global IPv6 prefix.
  - **Allow User to Specify Netmask**: Select this to allow users to specify the subnet mask when creating networks using this template.
- **Comment**: Enter useful information about the template.
- **Automatically create a reverse-mapping zone**: This function is enabled if the fixed netmask of the template is a multiple of 4 (4, 8, 24, and so on), or if you select the **Allow User to Specify Netmask** option. Select this if you want the appliance to automatically create the corresponding reverse-mapping zone for the networks created using this template. These zones are created in the DNS view assigned to receive dynamic DNS updates at the network level.

The **Cloud** section appears when the Cloud Network Automation license is installed on the Grid Master. For information, see **Deploying Cloud Network Automation**. To configure this template for cloud delegation, complete the following:

**Use for cloud delegation**: Select this check box to enable cloud delegation for this template.

**Delegate authority from the Grid Master**

- **Delegate To**: In a non-cloud API request, this parameter defines the default member to which authority is delegated. In a cloud API request, the appliance ignores this parameter, which allows you to use this template to create an object on different Cloud Platform Appliances. Click Select to choose the default Cloud Platform Appliance to which you want to delegate authority. The **Member Selector** displays only Cloud Platform Appliances in the Grid. Click the member, and Grid Manager displays the member name next to this field.

4. Click Next to associate Active Directory Sites with the network. For more information, see **Associating Active Directory Sites with Networks**.

5. Click Next to assign Grid members to this network template. Ensure that you include members that are associated with other templates that you plan to add to this network template. You can assign one or multiple members to this template. However, you cannot assign a combination of NIOS Grid members and vNIOS Grid members to the template.

- Click the Add icon to add a Grid member as a DHCP server for the networks created using this template. Select the Grid member from the **Member Selector** dialog box. Keep in mind, DHCP properties for the network are inherited from this member. Networks created using this template can be served by multiple members, but a member can serve networks in one network view only.

6. Click Next, and then click the Add icon to include DHCP range and fixed address templates in the network template. Choose the template that you want to include in this network template. Use **SHIFT-click** and **CTRL-click** to select multiple templates.

You can remove a template from the list by selecting the template and clicking the **Delete** icon.

7. Click Next to configure or override DHCP options as described in **Defining General IPv6 Properties**.

8. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see **Using Extensible Attributes**.

If you are adding an RIR network, the RIR network attribute table appears. For information about these attributes and how to enter them, see **RIR Network Attributes**.

9. Save the configuration.

**Modifying IPv6 Network Templates**
To modify and set the properties of a network template:

1. From the Data Management tab, select the DHCP tab -> Templates tab -> template check box, and then click the Edit icon.
2. The Network Template editor contains the following tabs from which you can modify data:
   - **General**: Modify general information described in 4823811
   - **Member Assignment**: Change the Grid members that provide DHCP services for networks created from this template. For information, see Adding IPv6 Networks.
   - **Templates**: Add or delete DHCP range and fixed address templates. For information, see Adding IPv6 Range Templates and Adding IPv6 Fixed Address Templates.
   - **IPv6 DHCP Options**: Keep the inherited DHCP options or override them and enter unique settings for the template. For information, see Defining General IPv6 Properties.
   - **RIR Registration**: Modify RIR network information. This tab appears only when support for RIR updates is enabled. For information, see Modifying RIR Network Data.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with the template. You can also modify the values of the extensible attributes. For information, see Using Extensible Attributes.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify data:
   - **IPv6 DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the template. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration.

**Viewing Templates**

To view a list of all IPv4 and IPv6 DHCP templates:

1. From the Data Management tab, select the DHCP tab -> Templates tab.
2. Grid Manager displays the following information:
   - **Name**: The name of the template.
   - **Type**: The template type, such as IPv4 Network Template or IPv6 Network Template.
   - **Comment**: The information you entered about the template.
   - **Site**: The site to which the template belongs. This is one of the predefined extensible attributes.

You can select predefined and user defined extensible attributes for display. You can also do the following in this panel:

- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
- Sort the displayed data in ascending or descending order by column.
- Delete a selected template or multiple templates. For information, see Deleting Templates.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Select an object and edit its information.
- Print or export the data in the panel.

**Deleting Templates**

To delete a template:

1. From the Data Management tab, select the DHCP tab -> Templates tab -> template check box, and then click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes.
Chapter 29 Managing IPv6 DHCP Data

This chapter explains how to configure and manage IPv6 DHCP data. It contains the following sections:

- **Configuring IPv6 Networks**
- **Defining Global IPv6 Prefixes**
- **Managing IPv6 Networks**
  - Adding IPv6 Networks
  - Modifying IPv6 Networks
  - Deleting IPv6 Networks
- **About IPv6 Shared Networks**
  - Adding IPv6 Shared Networks
  - Modifying IPv6 Shared Networks
  - Deleting IPv6 Shared Networks
- **Configuring IPv6 Address Ranges**
  - Adding IPv6 Address Ranges
  - Setting the Priority of IPv6 Address Ranges
  - Modifying IPv6 Address Ranges
  - Deleting IPv6 Address Ranges
- **Configuring IPv6 Fixed Addresses**
  - Adding IPv6 Fixed Addresses
  - Modifying IPv6 Fixed Addresses
  - Deleting IPv6 Fixed Addresses
- **Viewing IPv6 DHCP Objects**

### Configuring IPv6 Networks

To configure DHCP services for an IPv6 network and the resources in the network, perform the following tasks:

1. To facilitate network creation, you can specify the IPv6 global prefixes for the Grid. For more information, see [Defining Global IPv6 Prefixes](#).
2. Create a network and assign it to Grid members. For information, see [Managing IPv6 Networks](#) and [About IPv6 Shared Networks](#).
3. Optionally, configure DHCP properties for the network. You can override properties set at the Grid or member level and enter unique values for the network and fixed addresses. For information, see [Configuring DHCPv6 Properties](#) and [Configuring DHCP IPv4 and IPv6 Common Properties](#).
4. Optionally, assign zones to a network. For information, see [Associating Networks with Zones](#).
5. Add a DHCP range to the network and assign it to a member. For information, see [Configuring IPv6 Address Ranges](#).
6. Optionally, add exclusions to the DHCP range for addresses that are not used for dynamic allocation. For information, see [Modifying IPv6 Address Ranges](#).
7. Optionally, configure DHCP properties for the address range. You can override properties set at an upper level and enter unique values for the address range. For information, see [Modifying IPv6 Address Ranges](#).
8. Optionally, add fixed addresses to the network and configure DHCP properties for them. A fixed address may also be associated with a device port through a Port Reservation. For information, see [Configuring IPv6 Fixed Addresses](#).
9. Start the DHCP service and the IPv6 DHCP service. For more information, see [Starting DHCP Services on a Member](#).

### Defining Global IPv6 Prefixes

To simplify network creation, you can define IPv6 prefixes that are used for networks served by the Grid members. If your organization is assigned IPv6 prefixes, you can enter them globally at the Grid level, and then just select the appropriate IPv6 prefix when you define the network and network templates. You can create multiple global prefixes. When you define an IPv6 network and network templates, you must adjust the slider to the desired netmask as per the CIDR in the prefix. Use the netmask slider to select /64 as the CIDR, if an IPv6 prefix is unavailable for an IPv6 network.

To add global IPv6 prefixes:

1. From the **Data Management** tab, select the **DHCP** tab.
2. Expand the Toolbar and click **Grid DHCP Properties**.
3. In the **Grid DHCP Properties** editor, select the **IPv6 Global Prefixes** tab.
4. Click the Add icon and enter a name for the prefix and the prefix. Select the **Default** check box to specify a default IPv6 prefix for the Grid.
5. Save the configuration.

### Managing IPv6 Networks

You can create an IPv6 network from scratch or create a network template and then use that template to create one or more networks. Using a
network template facilitates creating multiple IPv6 networks with similar properties. You can also create an IPv6 network from the Tasks Dashboard. For information about the Tasks Dashboard, see The Tasks Dashboard.

An IPv6 network inherits its DHCP options & DDNS settings from its shared network, if it is part of a shared network, or from the member to which it is assigned.

If you have enabled support for RIR (Regional Internet Registry) updates and are adding an RIR IPv6 network container or network to NIOS, Grid Manager displays an RIR section in the Add IPv6 Network wizard. You must enter RIR related information in this section in order for NIOS to associate the newly added network with an RIR organization. For more information about RIR address allocation and updates, see RIR Registrations and Updates.

Adding IPv6 Networks

To add an IPv6 network:

1. Select the Data Management tab.
2. If you have more than one network view in the system, select the network view in which you want to add the network.
3. Select the DHCP tab -> Networks tab.
4. In the Networks section, click the Add drop-down list and select IPv6 Network.
5. In the Add IPv6 Network wizard, select one of the following and click Next:
   - Add IPv6 Network: Click this to add an IPv6 network from scratch.
   - Add IPv6 Network using Template: To use a template, click this, and then click Select Template and select an IPv6 network template. For information about network templates, see About IPv6 Network Templates. When you use a template to create a network, the configurations of the template apply to the new network. The appliance populates the template properties in the wizard when you click Next. You can then edit the pre-populated properties. If the template specified a fixed netmask, you cannot edit the netmask.
6. Complete the following and click Next:
   - Regional Internet Registry: This section appears only when support for RIR updates is enabled. For information about RIR, see RIR Registration Updates. Complete the following to create an RIR IPv6 network container or network:
     - Internet Registry: Select the RIR from the drop-down list. The default is RIPE. When you select None, the network is not associated with an RIR organization.
     - Organization ID: Click Select Organization and select an organization from the RIR Organization Selector dialog box.
     - Registration Status: The default is Not Registered. When adding an RIR allocated network, you can change this to Registered and select the Do not update registrations check box below. Note that when you select API as the communication method, the registration status will be updated automatically after the registration update is completed. However, when you select Email as the communication method, the registration status will not be automatically updated. If you are creating a new network and the registration update is completed successfully, the status will be changed to Registered. If the update fails, the status will be changed to Not Registered. The updated status and timestamp are displayed in the Status of last update field in the IPv6 Network Container or IPv6 Network editor.
     - Registration Action: Select the registration action from the drop-down list. When you select Create, the appliance creates the IPv4 network and assigns it to the selected organization. When you select None, the appliance does not send registration updates to RIPE. When you are adding an existing RIR allocated network to NIOS, select None. When you are adding networks to an RIR allocated network (a parent network), select Create. Ensure that the parent network associated with an RIR organization already exists.
     - Do not update registrations: Select this check box if you do not want the appliance to submit RIR updates to RIPE. By default, the appliance sends updates to the RIR database based on the configured communication method.
   - Network View: This appears only when you have multiple network views. From the drop-down list, select the network view in which you want to create the network.
   - Netmask: Use the netmask slider to select the appropriate number of subnet mask bits for the network. Select /64 as the CIDR, if an IPv6 prefix is unavailable for an IPv6 network. When the prefix is available, you must adjust the slider to the desired netmask as per the CIDR in the prefix.
   - Networks: Do one of the following to add new networks:
     - Click the Add icon to enter a new network. If you are adding a network for a previously defined global IPv6 prefix, you can select the prefix from the IPv6 Prefix drop-down list. The default is None, which means that you are not creating an IPv6 network for a previously defined subnet route. If you have defined a global prefix at the Grid level, the default is the global prefix value. Click Add and Grid Manager adds a row to the table. Enter the network address in the Network field. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2001:0db8:0000:0000:0000:0000:0102:0304 can be shortened to 2001:db8::0102:0304. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The appliance displays an IPv6 address in its shortened form, regardless of its form when it was entered. Click Add again to add another network. You can also select a network and click the Delete icon to delete it.
     - or
     - Click the Next Available icon to have the appliance search for the next available network. Complete the following in the Next Available Networks section:
       - Create new network(s) under: Enter the network container in which you want to create the new network. When you enter a network that does not exist, the appliance adds it as a network container. When you enter a network that is part of a parent network, the parent network is converted into a network container if it does not have a member assignment or does not contain fixed addresses and host records that are served by DHCP. You can also click Select Network to select a specific network in the Network Selector dialog box. For information about how the appliance searches for the next available network, see Obtaining the Next Available.
Number of new networks: Enter the number of networks you want to add to the selected network container. Note that if there is not enough network space in the selected network to create the number of networks specified here, Grid Manager displays an error message. The maximum number is 20 at a time. Note that when you have existing networks in the table and you select one, the number you enter here includes the selected network.

Click Add Next to add the networks. Grid Manager lists the networks in the table. You can click Cancel to reset the values.

Note: You must add the network container you enter in the Next Available Networks section. If you enter a network in the Next Available Networks section and then use the Add icon to add another network, the appliance does not save the network you enter in the Next Available Networks section until you click Add Next.

- Comment: Enter additional information about the network, such as the name of the organization it serves.
- Automatically create reverse-mapping zone: This function is enabled if the netmask of the network is a multiple of four, such as 4, 8, 12 or 16. Select this to have the appliance automatically create reverse-mapping zones for the network. A reverse-mapping zone is an area of network space for which one or more name servers have the responsibility for responding to address-to-name queries. These zones are created in the DNS view assigned to receive dynamic DNS updates at the network view level.
- Disable DHCP: Select this if you do not want the DHCP server to provide DHCP services for this network at this time. This feature is useful when you are in the process of setting up the DHCP server. Clear this after you have configured the server and are ready to have it serve DHCP for this network.

The Cloud section appears when the Cloud Network Automation license is installed on the Grid Master. For information, see Deploying Cloud Network Automation. To delegate authority for this network, complete the following:

Delegate authority from the Grid Master

- Delegate To: This field indicates whether the authority for the network you want to create has already been delegated to a Cloud Platform Appliance. Click Select to choose the Cloud Platform Appliance to which you want to delegate authority. The Member Selector displays only Cloud Platform Appliances in the Grid. Click the member, and Grid Manager displays the member name next to this field. This cloud member now assumes authority for this network, and the Grid Master does not have authority any more. You can also click Clear to remove authority delegation from the selected Cloud Platform Appliance and return authority back to the Grid Master.

7. Click Next and add one or more Grid members as DHCP servers for the network.

- click the Add icon and select a Grid member from the Member Selector dialog box. Keep in mind, some DHCP properties for the network are inherited from this member. The network can be served by multiple members, but a member can serve networks in one network view only.

8. Click Next to associate Active Directory Sites with the network. For more information, see Associating Active Directory Sites with Networks.

9. (Applies only to Network Insight) Click Next to initiate or disable discovery of the new network(s). Discovery settings differ based on whether you are defining one network or multiple networks.

- Configuring one network: discovery settings include the following: Enable Discovery and Immediate Discovery, selecting a Probe member to perform the discovery; and Polling Options, which define how the network will be discovered by the Probe member. By default, all Polling Options discovery settings are inherited from the parent network (or Grid, if no parent exists) unless you click Override. Polling Options govern the protocols used to query and collect information about the network devices being discovered.

- Configuring more than one network: If the networks are child networks, they automatically inherit the settings of the parent network, including discovery settings and the discovery member. These settings will not appear in the wizard page. For discovery of multiple networks, you can only enable or disable Immediate Discovery. Click Next to override the DHCP properties described in Defining General IPv6 Properties.

10. As part of creating a network, you can provision the network on an actual device (switch, router, or switch-router), that is discovered and managed through the Grid Manager.

- Begin by checking the Enable Network Provisioning check box, and clicking the Select Device button. Choose your device from the Device Selector dialog. (Click Clear to remove the setting. For more information, see the section Using the Device Selector.)
- If you performed DHCP configuration in the previous step of the Add Network Wizard, the Router IP value will automatically be populated with the DHCP Router IP address value. Otherwise, you enter the standard router IP address.
- If required for the newly provisioned network to ensure that attached devices receive DHCP configuration, enable the DHCP Forwarding check box. For this setting, if a DHCP Failover was previously configured, the IP addresses defined for DHCP failover are automatically used for the DHCP forwarding configuration.
- You will also need to choose an interface on the selected device on which to provision the network by selecting it from the Interface drop-down menu. Grid Manager ensures that only those interfaces that can support provisioning, and are available for provisioning (that do not have an Operation Status of Up), appear in the drop-down menu.
- Otherwise, when creating networks and provisioning them on managed devices, you can create a VLAN on which to provision the network by clicking the Create VLAN option and entering the VLAN Name and VLAN ID. Ensure that the VLAN ID value you enter is appropriate for the application - don't create a new VLAN and provision a network for a VLAN value that is already actively carrying traffic for another routing domain.

If a selected device does not support VLANs, the Create VLAN option will not appear.
11. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see About Extensible Attributes.

If you are adding an RIR network, the RIR network attribute table appears. For information about these attributes and how to enter them, see RIR Network Attributes. You can preview the information before the appliance submits updates to the RIPE database. To preview registration updates, click Preview RIR Submissions. For more information, see Previewing Registration Updates.

**Note:** You cannot leave an optional RIR attribute value empty. If you do not have a value for an RIR attribute, you must delete it from the table. You can enter up to 256 characters for all RIR attributes.

12. As the final step in the Add IPv6 Network wizard, you define when Grid Manager creates the new network by scheduling it. You also schedule when the associated port control task executes (if a port configuration has been specified).

- To create the new network and its associated port configuration immediately, select **Now**. Grid Manager synchronizes the port control task to take place at the same time as the creation of the new network.
- You can choose to have Grid Manager execute the port control task at the same time as the network creation. To do so, select **At the same time as above**.
- You can choose to have Grid Manager execute the port control task at a later time by selecting **Later**. Choose a **Selected time** by entering or selecting a **Start Date** (click the calendar icon to choose a calendar date) and a **Start Time**, and choose a **Time Zone**.

13. Choose one of the following from the **Save &...** drop-down button menu:

- **Click Save & Close** to add the new network and close the wizard (this is the default).
- **Click Save & Edit** to add the new network and launch the editor.
- **Click Save & New** to add the new network and launch the wizard again to add another network.

**Note:** At any step during the wizard, you can click **Schedule for Later** to schedule the task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

After you create a network, you can do the following:

- Add it to a shared network. For more information, see Adding IPv6 Shared Networks.
- Use the split network feature to create subnets for the network. For information, see Splitting IPv6 Networks into Subnets.
- Use the join networks feature to create a parent network that encompasses multiple subnets into a larger network. For information, see Joining IPv6 Networks. You can also create a shared network for subnets that are on the same network segment.
- View a list of networks. For more information, see Viewing Networks.

Modifying IPv6 Networks

You can modify existing network settings and override the Grid or member DHCP properties, with the exception of the network address and netmask.

To modify an IPv6 network:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** check box, and then click the **Edit** icon.
2. The **IPv6 Network** editor contains the following basic tabs from which you can modify data:
   - **Generate Basic:** You can modify the following fields:
     - **Comment:** The information you entered for the network.
     - **Disabled:** This field is displayed only if the selected network is a network without a child network under it. You can disable and enable existing networks instead of removing them from the database, if the selected network does not have a child subnet. This feature is especially helpful when you have to move or repair the server for a particular network.

When the Cloud Network Automation license is installed on the Grid Master, Grid Manager displays the following information in the Cloud section: **Cloud Usage**, **Owned By**, and **Delegated To**. You cannot modify these fields. For more information, see 4817189.

- **Member Assignment:** Add or delete a Grid member that provides DHCP services for this network.
- **IPv6DHCPOptions:** Keep the inherited DHCP properties or override them and enter unique settings for the network. For information, see Defining General IPv6 Properties.
- **Discovery:** Checking the Enable Discovery check box informs NIOS to begin discovering the network after you click **Save and Close**. You manage discovery polling settings local to each network from this page. For a complete overview of features on this page, see Discovering Devices and Networks and its subsections.
- **Discovery Exclusions:** IP Addresses and IP ranges can be locally excluded from discovery by clicking the Add icon and selecting **Add IP Address** or **Add IP Range**. These IP addresses or IP ranges are selected from within the chosen network. For related information, see Excluding IP Addresses from Discovery and its subsections.
- **Discovery Blackout:** Define extended time periods and regularly scheduled times when discovery and/or port configuration tasks will not take place on a network. Editing a network under DHCP, blackout settings apply only to the specified network. You also specify the scheduled time when the blackout period begins, and the duration of the blackout period. By default, the network inherits its discovery blackout settings from the Grid level. For related information, see Defining Blackout Periods and its subsections.
Note: Discovery blackout settings also can be defined for DHCP ranges.

- **RIR Registration**: Modify RIR network information. This tab appears only when support for RIR updates is enabled. For information, see Modifying RIR Network Data.
- **Extensible Attributes**: Add and delete extensible attributes that are associated with a specific network. You can also modify the values of the extensible attributes. For information, see About Extensible Attributes.
- **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify advanced data.

   - **General Advanced**: You can associate zones with a network. For information, see Associating Networks with Zones.
   - **IPv6 DDNS**: Keep the inherited DDNS settings or override them and enter unique settings for the network. Note that you must click **Override** and select **Enable DDN Updates** for the DDNS settings you configure in this tab to take effect. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients.

Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration or click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

### Deleting IPv6 Networks

When you delete a network, all of its data, including all DHCP records, subnets, and records in its subnets, is deleted from the database. Because of the potentially large loss of data that can occur when you delete a network, the appliance stores the deleted network in the Recycle Bin. You can restore a deleted network from the Recycle Bin, if enabled. You can also disable a network instead of deleting it. For information, see 481718.

To delete a network:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> network check box, and then select **Delete** or **Schedule Delete** from the Delete drop-down menu.
2. To delete the network now, in the Delete Confirmation dialog box, click **Yes**. To schedule the deletion, see Scheduling Deletions.

The appliance puts the deleted network in the Recycle Bin, if enabled.

### About IPv6 Shared Networks

You can combine two or more contiguous IPv6 networks into a shared network. When you do, the DHCP server allocates IP addresses from both subnets. To create a shared network, create the individual subnets, and then create the shared network and add the subnets to it. For more information about shared networks, see About Shared Networks.

### Adding IPv6 Shared Networks

To add an IPv6 shared network:

1. Select the **Data Management** tab.
2. If you have more than one network view in the system, select the network view in which you want to add the network.
3. Select the **DHCP** tab -> **Networks** tab.
4. In the Shared Networks section, select IPv6 Shared Network from the Add drop-down menu.
5. In the Add IPv6 Shared Network wizard, do the following:
   - **Name**: Enter the name of the shared network.
   - **Comment**: Enter information about the shared network.
   - **Disabled**: Select this if you want to enable the shared network at a later time. You can disable and enable existing networks instead of removing them from the database. This feature is especially helpful when you have to move or repair the server for a particular network.
6. Click **Next** and do the following to add networks:
   a. Click the Add icon.
   b. In the Network Selector, select the networks that you want to include in the shared network. Ensure that the networks are served by the same Grid members to avoid DHCP inconsistencies.
7. Click **Next** to configure DHCP properties described in Defining General IPv6 Properties.
8. Click **Next** to enter values for required extensible attributes or add optional extensible attributes for the shared network. For information, see Using Extensible Attributes.
9. Save the configuration or click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

For information on viewing shared networks, see Viewing Shared Networks.

### Modifying IPv6 Shared Networks

To modify a shared network:
1. From the Data Management tab, select the DHCP tab -> Networks tab -> Shared Networks section -> shared_network check box, and then click the Edit icon.

2. The IPv6 Shared Network editor contains the following tabs from which you can modify data:
   - General: Modify the fields Name, Comments, and Disabled as described in 4817184
   - Networks: Displays the networks that are currently assigned to the shared network. You can add or delete a network.
   - To add a network, click the Add icon. To delete a network, select the network check box, and then click the Delete icon.
   - IPv6 DHCP Options: Keep the inherited DHCP properties or override them and enter unique settings for the shared network.
     For information, see Defining General IPv6 Properties.
   - Extensible Attributes: Add and delete extensible attributes that are associated with a specific network. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.
   - Permissions: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions.

3. Optionally, you can click Toggle Advanced Mode to display the following tabs from which you can modify advanced data.
   - IPv6 DDNS: Keep the inherited DDNS settings or override them and enter unique settings for the shared network. Note that you must click Override and select Enable DDNS updates for the DDNS settings you configure in this tab to take effect. For information, see Enabling DDNS for IPv4 and IPv6 DHCP Clients.

   Note that Grid Manager displays both the basic and advanced tabs the next time you log in to the GUI.

4. Save the configuration and click Restart if it appears at the top of the screen.

   or

   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

Deleting IPv6 Shared Networks

Though you can delete the networks in a shared network, a shared network must have at least one network in it. To delete a shared network:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Shared Networks section -> shared_network check box, and then select Delete or Schedule Delete from the drop-down menu.

2. To delete the shared network now, in the Delete Confirmation dialog box, click Yes. To schedule the deletion, see Scheduling Deletions.

   The appliance puts the deleted shared network in the Recycle Bin, if enabled.

Configuring IPv6 Address Ranges

You can configure IPv6 ranges that are used to delegate IPv6 prefixes only, to assign IPv6 addresses only, or to delegate IPv6 prefixes and assign IPv6 addresses. When you define a DHCP range to delegate prefixes, the prefixes can be outside of the network where they are being defined. IPv6 ranges inherit their properties from their network, so each range in a subnet provides the same set of options to their DHCP clients. Note that when an Infoblox DHCP server grants IPv4 leases, it starts from the last IP address in the range to the first. When the server grants IPv6 leases, it uses an algorithm based on the DUID of the client.

Adding IPv6 Address Ranges

To add a an IPv6 address range:

1. Navigate to the IPv6 network to which you want to add an address range, and then select Range from the Add drop down menu.

   or

   From any panel in the DHCP tab, expand the Toolbar and click Add -> Range -> IPv6.

2. In the Add IPv6 Range wizard, select one of the following and click Next:
   - Add IPv6 Range: Select this to add an address range from scratch.
     or
   - Add IPv6 Range Using Template

   Click Select Template and select the template that you want to use. Note that when you use a template to create a DHCP range, the configurations of the template apply to the new range. The appliance automatically populates the address range properties in the wizard. You can then edit the pre-populated properties. For more information, see About IPv6 Range Templates.

3. Complete the following:
   - Network: Click Select Network. Grid Manager displays the network address here if you have only one network configured. When there are multiple networks, Grid Manager displays the Select Network dialog box from which you can select one. Specify one of the following:
     - Address: Select this if the address range is used to allocate IPv6 addresses only to DHCP clients, and then enter the start and end addresses in the range.
     - PrefixDelegated: Select this if the DHCP server uses this address range to delegate IPv6 prefixes only to DHCP clients. Enter
the start and end prefixes, and the prefix length.

- Both: Select this if the DHCP server delegates IPv6 prefixes and allocates IPv6 addresses from this range. Enter the start and end addresses in the range, and the start and end prefixes, and the prefix length.

Complete the following:

- **Name**: Enter a name for the address range.
- **Comment**: Enter additional information about the address range.
- **Disabled**: Select this if you want to save the configuration for the address range but do not want to activate the address range yet. You can clear this check box when you are ready to allocate addresses from this range.

The Cloud section appears when the Cloud Network Automation license is installed on the Grid Master. For information, see Deploying Cloud Network Automation. To delegate authority for this range, complete the following:

**Delegate authority from the Grid Master**

- **Delegate To**: This field indicates whether the authority for the range you want to create has already been delegated to a Cloud Platform Appliance. Click Select to choose the Cloud Platform Appliance to which you want to delegate authority. The Member Selector displays only Cloud Platform Appliances in the Grid. Click the member, and Grid Manager displays the member name next to this field. This cloud member now assumes authority for this range, and the Grid Master does not have authority any more. You can also click Clear to remove authority delegation from the selected Cloud Platform Appliance and return authority back to the Grid Master.

4. Click **Next** and select one of the following to provide DHCP services for the DHCP range:

- **None (Reserved Range)**: Select this if you want to reserve this address range for static hosts. Addresses in this range cannot be allocated as dynamic addresses. You can allocate the next available IP from this range to a static host. This is selected by default.
- **Grid Member**: Select this if you want a Grid member to serve DHCP for this DHCP range. Select a Grid member from the drop-down list. The drop-down list displays only the Grid members that are associated with the network to which the DHCP range belongs.

5. (Applies only to Network Insight) Click **Next** to initiate or disable discovery of the new DHCP range.

- **Configuring one network**: Discovery settings include the following: Enable Discovery and Immediate Discovery, selecting a Probe member to perform the discovery; and Polling Options, which define how the network will be discovered by the Probe member using SNMP and CLI credentials. By default, all Polling Options discovery settings are inherited from the parent network unless you click Override. Polling Options govern the protocols used to query and collect information about the network devices being discovered. See the section Configuring Discovery Properties for a complete description of discovery Polling Options.

6. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes.

7. Save the configuration and click **Restart** if it appears at the top of the screen.

or

Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

## Setting the Priority of IPv6 Address Ranges

The DHCP server allocates IP addresses from the configured DHCP ranges according to the order in which the ranges are listed. By default, ranges are listed according to their start addresses. You can move the ranges up and down in the list to change their order. For information about viewing DHCP ranges and other objects in a network, see Viewing IPv6 DHCP Objects.

To change the order of DHCP ranges in a network:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> network.
2. Expand the Toolbar and click Order DHCP Ranges.
3. In the Order DHCP Ranges dialog box, click the up and down arrows to move ranges up or down on the list. The Priority value changes accordingly. Click **OK** to save the configuration.

## Modifying IPv6 Address Ranges

To modify an IPv6 address range:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.
2. The DHCP Range editor contains the following basic tabs from which you can modify data:

   - **General**: Modify the fields, except the network address, as described in Adding IPv6 Address Ranges.

When the Cloud Network Automation license is installed on the Grid Master, Grid Manager displays the following information in
the Cloud section: Cloud Usage, Owned By, and Delegated To. You cannot modify these fields. For more information, see Adding IPv6 Address Ranges.

- **Member Assignment:** Modify the Grid member that provides DHCP services for the DHCP range as described in Adding IPv6 Address Ranges.
- **Discovery:** You can enable and change discovery settings for the IPv6 range at any time after creating the range. Discovery settings include the following: Enable Discovery and Immediate Discovery, selecting a Probe member to perform the discovery; and Polling Options, which define how the network will be discovered by the Probe member using SNMP and CLI credentials. By default, all Polling Options discovery settings are inherited from the parent network unless you click Override. Polling Options govern the protocols used to query and collect information about the network devices being discovered. See the section Configuring Discovery Properties for a complete description of discovery Polling Options.
- **Discovery Blackout:** Define extended time periods and regularly scheduled times when discovery and/or port configuration tasks will not take place on a network or DHCP range. Editing a network or range under DHCP, blackout settings apply only to the specified network or range. You also specify the scheduled time when the blackout period begins, and the duration of the blackout period. By default, the network inherits its discovery blackout settings from the Grid level. For related information, see Defining Blackout Periods and its subsections.
- **IPv6 DHCP Options:** Keep active leases in a deleted DHCP range. For more information, see Keeping Leases in Deleted IPv4 and IPv6 Networks and Ranges.
- **Extensible Attributes:** You can add and delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.
- **Permissions:** This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions.

3. Optionally, you can click **Toggle Advanced Mode** to display the following tabs from which you can modify advanced data.

- **Exclusion Ranges:** Configure a range of IP addresses that the appliance does not use to assign to clients. You can use these exclusion addresses as static IP addresses. For more information, see About Exclusion Ranges.

Note that Grid Manager displays both the basic and advanced mode tabs the next time you log in to the GUI.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

or
Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

### Deleting IPv6 Address Ranges

To delete an IPv6 address range:

- From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** -> **addr_range** check box, and then click the Delete icon.

### Configuring IPv6 Fixed Addresses

You can configure IPv6 fixed addresses with either an IPv6 address or prefix. You can assign prefix-based fixed addresses to routers so they can advertise the prefixes associated with a link. The fixed addresses also can be bound to interfaces on a network device, such as a switch or a router, that is discovered and managed under IPAM. DHCP hosts, in turn, use these prefixes to generate IP addresses using the stateless autoconfiguration mechanism defined in RFC 2462, IPv6 Stateless Autoconfiguration. You can also create IPv6 fixed addresses from the Tasks Dashboard. For information about the Tasks Dashboard, see The Tasks Dashboard.

**Note:** IPv6 fixed addresses do not support dynamic DNS updates.

### Adding IPv6 Fixed Addresses

**Note:** At any time during the wizard, you can click **Schedule for Later** to schedule the task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

To add an IPv6 fixed address:

1. Navigate to the network to which you want to add a fixed address, and then select **Fixed Address** from the Add drop down menu.
   or
   From any panel in the DHCP tab, expand the Toolbar and click **Add** -> **Fixed Address** -> **IPv6**.
2. In the **Add Fixed Address** wizard, select one of the following and click **Next**:
   - **Add IPv6 Fixed Address**
   - **Add IPv6 Fixed Address Using Template**
Click Select Template and select the template that you want to use. When you use a template to create a fixed address, the configurations of the template apply to the new address. The appliance automatically populates the fixed address properties in the wizard. You can edit the pre-populated properties.

3. In this panel, the displayed network address can either be the last selected network or the network from which you are adding the fixed address. If no network address is displayed or if you want to specify a different network, click Select Network. When there are multiple networks, Grid Manager displays the Select Network dialog box.

Specify one of the following:

- **Address**: to assign an IPv6 address to a fixed address. You can either enter an IPv6 address or select Next Available IP to obtain the next available IP address. Note that for Cloud Network Automation, Next Available IP is not available if the fixed address you want to create is within a delegated range.
- **Prefix Delegation**: to assign an IPv6 prefix. Enter the prefix and prefix length.
- **Both**: to assign an IPv6 prefix and address. Enter the IPv6 address, prefix, and prefix length.

Complete the following:

- **DUID**: Specify the DHCP Unique Identifier (DUID) of the DHCP client assigned to this fixed address.
- **Name**: Enter a name for the fixed address.
- **Comment**: Optionally, enter additional information.
- **Disabled**: Select this if you do not want the DHCP server to allocate this IP address at this time.

The Cloud section appears when the Cloud Network Automation license is installed on the Grid Master. For information, see Deploying Cloud Network Automation. This section displays the following information:

- **Cloud Usage**: This field indicates whether this object is associated with any specific cloud extensible attributes or within a scope of delegation. It can be one of the following:
  - **Cloud from adapter**: Indicates that this object has been created by a cloud adapter and it may or may not be within a scope of delegation at the moment.
  - **Cloud from delegation**: Indicates that this object is within the scope of delegation or the object itself defines a scope of authority delegation, and it is not created by a cloud adapter.
  - **Used by cloud**: Indicates that this network or network container is associated with the extensible attribute Is External or I Share d and the value is set to True, which implies the network is a private or shared network managed by the CMP, and it is not Cloud from adapter or Cloud from delegation.
  - **Non-cloud**: The object is a regular NIOS object and is not within the scope of any authority delegation nor is it associated with any of these extensible attributes: Cloud API Owned, Is External or Is Shared. NIOS admin users can modify this object based on their permissions.
  - **Owned By**: A cloud object can be owned by the Grid Master or the cloud adapter. When the object is created by the Grid Master, this shows Grid. If the object is created by the cloud adapter, this shows Adapter.

Delegate authority from the Grid Master

- **Delegate To**: This field indicates whether the authority for the object you want to create has already been delegated. If so, it displays the name of the delegation.

4. Click Next to configure or override DHCP options as described in Defining General IPv6 Properties.

5. **(Applies only with Network Insight) This step is not required for creating a new Fixed Address.** In the current Wizard step, you can optionally define the following identification values and settings for the new object's port reservation:

- **Choose the Device Type**: Router, Switch-Router, Switch, MSFT (Microsoft) Server, NetMRI, NIOS, VNios, or ESX (VMware) Server.
  - The values on this page are not required for defining the actual port reservation in a later wizard step.
  - Certain device types could be descriptively relevant based on the type of object you are creating. As an example, the MSFT Server designator helps identify the new object as a Microsoft Hyper-V Host. The ESX Server designator can be used to identify the new object as a VMware ESX Host. These values are not required and will not affect the functionality of the object.

- **Choose the Device Vendor**: Cisco, Juniper, Aruba, Dell, Infoblox, or HP.

- You can also enter a Location and a Description. These values are advisory and not required for configuration.

  After you define this group of settings, you will still need to define a device port reservation, which is done in a later step.

6. Click Next to initiate or disable discovery of the new Fixed Address. **(Applies only to Network Insight) This step is not required for creating a new Fixed Address.**

   a. Choose either Exclude from Network Discovery or Enable Immediate Discovery. If you choose to Exclude, discovery will not execute on the Fixed Address. If you choose Enable Immediate Discovery, discovery will execute on the host after you save your settings. You may also choose to leave both options disabled.

   b. By default, the new fixed address object inherits its SNMP credentials from those defined at the grid level. Should you wish to override them for a local set of credentials, check the Override Credentials check box and select the SNMPv1/SNMPv2 or SNMPv3 option and enter the locally used credentials.

   c. You may also test the entered SNMP credentials by clicking Test SNMP Credential.

**Note**: For descriptions of SNMP credentials for discovery, see the section Configuring SNMPv1/v2 Credentials for Polling and Configuring SNMPv3 Properties. These Grid-based values are inherited, by default, by each new object you create.
For the new object, you can check the **Override CLI Credentials** check box to override the inherited set of CLI credentials taken from the Grid level. This set of credentials may be used for the device that is directly associated with the new object in its Port Reservation.

You can also click **Test CLI Credentials** to enter and test a set of CLI login credentials against a device based on its IP address. Port control operations require CLI credentials for the involved devices. (If you are not using port control for the new object, usage of CLI credentials is optional.) Because some IPAM and DHCP objects will use port control features as part of object creation, CLI credentials are automatically leveraged as part of discovery. Ensure you have the correct sets of CLI credentials for devices in your network. See the section Configuring CLI Discovery Properties for related information.

SSH is the default for CLI operations. Check the **Allow Telnet** check box if you know the device involved in the object assignment may support Telnet but may not support SSH, or if you want Telnet as an option.

**Note:** All port control operations require CLI credentials to be entered into Grid Manager. Because some IPAM and DHCP objects will use port control features as part of object creation, CLI credentials are automatically leveraged as part of discovery. Ensure you have the correct sets of CLI credentials for devices in your network.

7. Click **Next** to define the port reservation for the device port that will be associated with the new Fixed Address. *This step is not required for creating a new Fixed Address.* This feature set is also termed **port control** in the NIOS/Grid Manager system. The device to which the new Fixed Address will be associated should already be discovered and managed from the Grid Manager.

- Begin by checking the **Reserve Port** check box. Note that reserving a switch port does not guarantee its availability. Optionally, you can skip connecting port configuration by clicking **Next**.
- Click the **Clear** button to remove the selected device from the configuration.
- Click the **Select Device** button to choose the device for which the port reservation will be associated. You should know the identity of the device to whose interface the new object will be associated before taking this step. For more information, see the section Using the Device Selector.
- After choosing the device, choose the **Interface** with which the port reservation will be bound. The drop-down list shows only interfaces that are most recently found to be available by Grid Manager during the last discovery cycle. This list will not include any ports that are Administratively Up and Operationally Up, or that are otherwise already assigned to other networks or objects.
- The Wizard page also shows a list of any VLANs that are currently configured in the chosen device (**The following VLANs are configured**). This Wizard page allows only the assignment of an existing VLAN in the chosen device to the new port reservation.
- Check the **Configure Port** check box to define specific port control settings for the port reservation.
- Choose the **Data VLAN** and/or the **Voice VLAN** settings you may need for the port assignment. Depending on the selected device, you may or may not be able to apply VLAN settings.
- Set the **Admin Status** to **Up** if you need to activate the port after assignment in the current task.

All port control operations require CLI credentials to be entered into Grid Manager. Because some IPAM and DHCP objects will use port control features as part of object creation, CLI credentials are automatically leveraged as part of discovery and definition of port configurations such as Admin Up/Down status. Ensure you have the correct sets of CLI credentials for devices in your network.

8. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes.

9. As the final step in the Add Fixed Address wizard, you define when Grid Manager creates the new object by scheduling it. You also schedule when the associated port configuration task executes.

- To create the new object and its associated port configuration immediately, select **Now**. The port control event is automatically synchronized to take place at the same time as the activation of the new object.
- You can choose to have Grid Manager execute the port reservation task at the same time as the Fixed Address object creation. To do so, select **At same time as Host**.
- You can choose to have Grid Manager execute the port reservation task at a later time by selecting **Later**. Choose a Selected time by entering or selecting a **Start Date** (click the calendar icon to choose a calendar date) and a **Start Time**, and choose a **Time Zone**.

10. Choose one of the following from the **Save &...** drop-down button menu:

- Click **Save & Close** to add the new object and close the wizard (this is the default).
- Click **Save & Edit** to add the new object and launch the editor.
- Click **Save & New** to add the new object and launch the wizard again to add another Fixed Address object.

11. Save the configuration and click **Restart** if it appears at the top of the screen.

**Note:** At any step during the wizard, you can click **Schedule for Later** to schedule the task. In the **Schedule Change** panel, enter a date, time, and time zone. For information, see Scheduling Tasks. You cannot schedule this task when you are creating an object that is within a delegated scope.

For information on viewing IPv6 fixed addresses in a network, see Viewing IPv6 DHCP Objects.
Modifying IPv6 Fixed Addresses

To modify a fixed address:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network -> fixed_address check box, and then click the Edit icon.
2. The Fixed Address editor contains the following basic tabs from which you can modify data:
   - **General:** You can modify all the fields you filled out in the first step of the wizard described in Adding IPv6 Fixed Addresses.
   - **Device Information:** You can change advisory Device Information settings for the object's port reservation; settings are described in the section Configuring IPv6 Fixed Addresses.
   - **Discovery:** Checking the Enable Discovery check box informs NIOS to begin discovering the network after you click Save and Close. You manage discovery polling settings local to each fixed address from this page. For a complete overview of features on this page, see Discovering Devices and Networks and its subsections.
   - **Port Reservation:** Review and edit any device port reservations that may be defined for the current object, or create a new port reservation and schedule it. For a closer look, see the section Port Control Features in Network Insight, and steps 5-9 in the section Configuring IPv6 Fixed Addresses.
   - **IPv6 DHCP Options:** You can keep the inherited DHCP options or override them and enter unique settings for the fixed address. For information, see Defining General IPv6 Properties.
   - **Discovered Data:** You can view discovered data of this address, if any, in this tab. For information, see Viewing Discovered Data.
   - **Extensible Attributes:** Add and delete extensible attributes that are associated with a specific network. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.
   - **Permissions:** This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions.

3. Save the configuration and click Restart if it appears at the top of the screen.
   
   or

   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

Deleting IPv6 Fixed Addresses

To delete a fixed address, from the Data Management tab, select the DHCP tab -> Networks tab -> Networks section -> network -> fixed_address check box, and then click the Delete icon. You cannot delete multiple fixed addresses at the same time if the authority for one of the fixed addresses is delegated to a Cloud Platform Appliance.

Viewing IPv6 DHCP Objects

You can view the DHCP objects in an IPv6 network by navigating to the DHCP tab -> Networks tab -> Networks panel, and then clicking the network link. This panel displays the following information about DHCP objects in the selected IPv6 network:

- **IP Address:** The IPv6 address of a DHCP object, such as a DHCP range, fixed address, or host configured for DHCP, or roaming host with an allocated IP address. For a DHCP range, this field displays the start and end addresses of the range. For a host that has multiple IPv addresses, each IP address is displayed separately. Note that the appliance highlights all disabled DHCP objects in gray.
- **Type:** The DHCP object type, such as IPv6 DHCP Range or IPv6 Fixed Address.
- **Name:** The object name. For example, if the IP address belongs to a host record, this field displays the hostname.
- **Comment:** The information you entered for the object.
- **Site:** The site to which the DHCP object belongs. This is one of the predefined extensible attributes. You can select the following additional columns for display:
  - **Priority:** Displays the priority of the DHCP range.
  - **Disabled:** Indicates whether the network is disabled. You can also do the following in this panel:
    - Modify some of the data in the table. Double click a row, and either modify the data in the field or select an item from a drop-down list.
    - Click Save to save the changes. Note that some fields are read only.
    - Sort the data in ascending or descending order by column.
    - Create a bookmark for the object.
    - Click Go to IPAM View to view information about the object in the IPAM tab.
    - Delete or schedule the deletion of a selected object or multiple objects.
    - Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
    - Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- **Print or export the data.

Chapter 30 DHCP Failover
This chapter explains how to configure DHCP failover associations. It contains the following sections:

- **About DHCP Failover**
  - Failover Association Operations
- **Configuring Failover Associations**
  - Adding Failover Associations
  - Best Practices for Restoring Microsoft DHCP Server Data
- **Managing Failover Associations**
  - Modifying Failover Associations
  - Monitoring Failover Associations
  - Deleting Failover Associations
  - Setting a Peer in the Partner-Down State
  - Performing a Force Recovery
  - Recovering DHCP Failover Associations

### About DHCP Failover

You can create a failover association between two DHCP servers (a primary server and a secondary) and assign the failover association to serve an IPv4 DHCP range. When you set up a failover association, you greatly reduce DHCP service downtime if one of your DHCP servers is out of service. You can better manage IP address requests by making two servers available for DHCP services. You can also configure one of the servers to assume full DHCP services when you know the other server may go out of service for a period of time.

You can configure two NIOS appliances, or one appliance and one external server, to form a failover association. The pairing of a primary and secondary server is called a peer association. The failover peers establish a TCP connection for their communication. They share a pool of IP addresses that they allocate to hosts on their networks based on load balancing. Load balancing is a technique to split the address allocation workload evenly across the two DHCP servers. You can assign a DHCP failover association to serve DHCP ranges in a network. A DHCP failover association can serve DHCP ranges that belong to one network view only. It cannot serve ranges in different network views.

**Note:** When you assign a failover association to serve DHCP ranges and networks, NIOS denies dynamic BOOTP clients by default, regardless of whether you select or deselect the **Deny BOOTP Requests** option from Grid Manager. However, if the DHCP ranges or networks are assigned to a single DHCP server (not a failover association), NIOS does not automatically deny dynamic BOOTP clients. In this case, you must manually select the **Deny BOOTP Requests** option through Grid Manager to ensure that NIOS denies BOOTP requests to avoid problems such as receiving two IP addresses for the same network device. For information about how to deny BOOTP requests, see *Configuring IPv4 BOOTP and PXE Properties*.

### Failover Association Operations

When a host broadcasts a DHCPDISCOVER message, it includes its MAC address. Both the primary and secondary peers receive this message. To determine which server should allocate an IP address to the host, they each extract the MAC address from the DHCPDISCOVER message and perform a hash operation. Each server then compares the result of its hash operation with the configured load balancing split. The split is set to 50% by default to ensure an even split between the two servers. When the split is 50%, the primary server allocates the IP address if the hash result is between 1 and 127, and the secondary server allocates the IP address if the hash result is between 128 and 255. As a server allocates an IP address, it updates its peer so their databases remain synchronized.

As shown in Figure 30.1, when a host broadcasts a DHCPDISCOVER message, both the primary and secondary servers receive the message. They perform a hash operation on the MAC address in the DHCPDISCOVER message, and the result is 250. Since the load balancing split is 50% and the hash result is 250, the secondary server responds to the host with a DHCPOFFER message. The secondary peer allocates an IP address from its assigned pool of IP addresses. It then sends a lease update message to the primary server so that the primary server knows how the address is assigned and can properly take over if the secondary server fails.

*Figure 30.1 Load Balancing and IP Addresses Allocation*
Configuring Failover Associations

1. **Grid**: From the **Data Management** tab, select the **DHCP** tab, and then click **Grid DHCP Properties** from the Toolbar.

   Click **Toggle Advanced Mode** if the editor is in basic mode. When the additional tabs appear, select the **General Advanced** tab to complete the following:

   - **Failover Port**: You can modify the port number that members use for failover associations. You can use any available port from 519 to 647. The default is 647 for a new installation and 519 for an upgrade.

   The following are tasks and guidelines for configuring a DHCP failover:

   1. Identify the primary and secondary DHCP servers and ensure that the appliances are set up correctly for the failover association, using the following guidelines:
      - Configure a failover association using two NIOS appliances, or a NIOS appliance and an ISC DHCP compliant server.
      - One of the DHCP servers must be an independent appliance or in an Infoblox Grid.
      - The DHCP servers do not have to be in the same geographic location.
      - The clocks on both servers must be synchronized. This happens automatically when both servers are on the same Grid.
      - Both servers must use the same version of the DHCP configuration file. This happens automatically when both servers are on the same Grid.
      - If you use firewalls on your networks, ensure that the firewalls allow TCP port 519 between the servers, and that TCP port 7911 is open for partner down operations.
      - Each pair of DHCP servers can participate in only one failover association. An appliance can participate in more than one failover association, as long as it is with a different peer.

   Configure the same DHCP properties on the primary and secondary servers, as described in **Configuring General IPv4 DHCP Properties**.

   - Both the primary and secondary servers must have the same operational parameters, and they must be able to receive DHCPDISCOVER messages that hosts broadcast on the networks.
   - If you change any of the DHCP failover parameters for a peer association definition, you must make the same changes on both the primary and secondary servers.

   **Note**: If both the primary and secondary servers are in a Grid, you configure the properties on the failover association and the configuration applies to both servers.

2. Create a failover association and configure load balancing between the servers. For information, see **Adding Failover Associations**.

   - Ensure that you use the same failover association name on both the primary and secondary servers.
   - The appliance assigns default values to the failover timers and triggers. In general, these default values serve the purpose of a failover. Do not change these values unless you understand the ramifications of the changes. For example, when one of the peers in a failover association fails, the other peer goes into a COMMUNICATIONS-INTERRUPTED state, and the lease time changes to the MCLT (Maximum Client Lead Time). You should consider how the MCLT affects the lease time when a failover occurs if you want to change this value.

3. Assign the failover association to the DHCP ranges in the same network view. Failover associations can serve only IPv4 DHCP ranges. For information, see **Configuring IPv4 Address Ranges**.

   - If you configure a shared network, and the subnets in the shared network contain ranges served by a DHCP failover association, both the primary and secondary DHCP server must have the same shared networks defined, containing the same networks and DHCP ranges.
**Note:** If you have multiple networks that are in a shared network and you plan to use a DHCP failover, you must use the same failover association and specify the same peers on all the networks in the shared network.

4. Enable DHCP on the primary and secondary servers AFTER you complete all the configurations. For information, see [Managing Failover Associations](#).

**Note:** When you set up a failover association for the first time, ensure that both servers are up and running and their databases are synchronized before they can start assigning IP addresses.

When you configure a failover association, the appliance assigns default values for timers and triggers, such as the MCLT and the maximum number of "unasked" packets. A failover may occur when some of the timers expire or when a failover peer goes out of service. When a failover occurs, the functional peer takes over and assigns IP addresses with the lease time set to the MCLT. When the server that is offline comes back online, it synchronizes its database with its peer before it starts allocating IP addresses.

### Adding Failover Associations

To add a DHCP failover association, perform the following procedures on both the primary and secondary servers:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **IPv4 Failover Associations** section, and then click the **Add** icon.
   
   or Expand the Toolbar and click **Add** -> **IPv4 Failover Association**.

2. In the **Add Failover Association** wizard, complete the following:
   
   - **Name:** Enter a unique name for the failover association. The failover association name is case sensitive. Enter the same name on both the primary and secondary servers. The appliance validates the names on both servers. The names must be exactly the same. If they do not match, the failover association goes into disconnect mode.
   - **DHCP Failover Primary:** Select one of the following. The default is **Grid Member**.
     - **Grid Member:** Click **Select member**. In the **Select Member** dialog box, select the primary server and click the Select icon.
     - **MS Server:** Click **Select Server**. In the **Microsoft Server Selector** dialog box, select the Microsoft server that supports DHCP failover. Note that only certain versions of Microsoft servers support failover. This dialog box also displays the following columns: **IP address**, **Comment**, and **Site**. The failover association requires at least two Microsoft servers. NIOS displays an error message when you select **MS Server** if there is only one Microsoft server. When you add or modify a failover association through Grid Manager, the appliance displays a message to ensure the connectivity between two Microsoft servers. If you want a failover association to be in a normal state, you must ensure an end-to-end connectivity. If the connectivity fails, you must re-establish connectivity between the two Microsoft servers and the failover association follows the recovery states based on the DHCP failover protocol.

**Note:** You can configure Microsoft primary and secondary servers using this wizard only. You cannot edit Microsoft primary and secondary servers after you configure them. You must delete and reconfigure the primary or secondary Microsoft server for a failover association.

- **External Server IP Address:** Select this to use an external ISC DHCP compliant server as the primary server. Enter the IP address of the primary server in the field.
- **DHCP Failover Secondary:** Select one of the following. The default is **Grid Member**.
  - **Grid Member:** Click **Select member**. In the **Select Member** dialog box, select the secondary server and click the Select icon.
  - **MS Server:** NIOS selects this automatically when you set the **DHCP Failover Primary** to **MS Server**. Click **Select Server**. In the **Microsoft Server Selector** dialog box, select the Microsoft server that supports DHCP failover. Note that only Microsoft Windows Server 2012 or later versions support synchronization of failover relationships. This dialog box also displays the following columns: **IP address**, **Comment**, and **Site**.

**Note:** The primary and secondary Microsoft servers that you select in a failover relationship must be in the same network view. For more information, see [About Microsoft DHCP Failover Relationships](#).

- **External Server IP Address:** Select this to use an external ISC DHCP compliant server as the secondary server. Enter the IP address of the secondary server in the field.

**Note:** You cannot select **External Server IP Address** for both the primary and secondary servers. One of the servers must be an independent appliance or in an Infoblox Grid.

- **Comment:** Enter useful information about the failover association.

3. Click **Next** and do the following to control the IP address allocation between the peers and how they switch from one to the other based on the configuration:

   - **Failover mode:** This is valid for Microsoft Management only. Select a failover mode. You can either select **Hot standby** or **Load balancing**. When you select **Hot standby**, the secondary server is set to **Standby** by default and the slider move to the position.
at 95%. The slider moves to 50% when you set the failover mode to **Load balancing mode**. You can synchronize and manage a failover mode that is operating in **Hot standby** mode. The primary partner is the active server that first creates the relationship if you use the **Load balancing** or the **Hot standby** mode.

**Note:** When you configure a failover association, the slider changes its position based on the **Failover mode** you select. When you edit failover settings, the slider remains in the **Balanced** position, at 50%, by default. For more information about modifying failover associations, see *Modifying Failover Associations*.

- **Load Balancing Data:** Adjust the slider to determine which server should handle more IP address requests. The default is 50%. When you move the slider all the way to the left, the primary server responds to all IP address requests, and the secondary server does not respond to any. The opposite applies when you move the slider all the way to the right. Infoblox recommends that you use the default (50/50) to enable the primary and secondary servers to respond to IP address requests on an equal basis.
- **Lease Deletion:** Select the following to override settings at the Grid and member levels.
  - **Keep leases from deleted ranges until one week after expiration:** When you select this and delete a DHCP range with active leases, the appliance stores these leases up to one week after they expire. When you add a new DHCP range that includes the IP addresses of these active leases, the appliance automatically restores the leases.
- **Secondary role:** This is valid for Microsoft Management only. Note that the secondary role is available only in **Hot standby** mode. The appliance displays **Standby** by default and you cannot edit this value.
- **Maximum client lease time:** Specify the maximum client lease time in minutes or hours. The default is one hour. Select **Minutes** or **Hours** from the drop-down list. This specifies the maximum amount of time the server waits before assuming control.
- **Enable switchover interval:** This is valid for Microsoft Management only. Select this to automatically change the state to partner down after a specified period. NIOS does not support the "partner down" state for Microsoft DHCP failover association.
- **State switchover interval (Minutes):** This is valid for Microsoft Management only. Specify the amount of time after which the server must change the state. The default is 60 minutes.
- **Enable Authentication:** This is valid for Microsoft Management only. Select this if you want to secure the communication between failover partners.
- **Shared Secret:** This is valid for Microsoft Management only. Enter a shared secret that can be used to authenticate the communication between failover partners. You can specify a shared secret only if you enable authentication.

4. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes*.

5. Save the configuration and click **Restart** if it appears at the top of the screen.

**Best Practices for Restoring Microsoft DHCP Server Data**

When you synchronize two Microsoft servers in read/write mode for a Microsoft DHCP failover association, the appliance might override new data. For example, assume that you are synchronizing data from one Microsoft server, which has latest data. But after the restore operation, the appliance will synchronize data from a Microsoft server that has old data. If you synchronize old data, it might override new data. Infoblox recommends that you follow the steps mentioned below to prevent new data being replaced with the old one:

1. Disable DHCP synchronization for the Microsoft server before you restore data to the Microsoft server.
2. Restore the Microsoft DHCP server.
3. From the Microsoft server, which has the latest data, replicate its DHCP failover association and scopes to the restored Microsoft server. This ensures that both Microsoft servers have the same latest data.
4. Re-enable DHCP synchronization for the restored Microsoft server. NIOS will resynchronize with the Microsoft server.

**Managing Failover Associations**

After you establish a failover association, you can monitor its status periodically to ensure that it is functioning properly. You can also delete a failover association when it is not assigned to any DHCP range. See the following sections on how to manage failover associations:

- 4823839
- 4823839
- 4823839

Under special circumstances, you can manually adjust the configuration of a failover association. For example, when you know in advance that a peer will be out of service for an extended period of time, you can manually set the functional peer in a PARTNER-DOWN mode. This allows the functional partner to assume all leases and be able to allocate addresses to client requests in full capacity. In addition, when you suspect the databases in a failover association are not synchronized, you can consider doing a force recovery (after you consult with Infoblox Technical Support or your Infoblox representative) so the secondary server can completely rebuild its lease table with updates from the primary server. See the following sections on how to set a peer to the partner-down mode and perform a force recovery:

- 4823839
- 4823839
Modifying Failover Associations

To modify a failover association:

1. From the Data Management tab, select the DHCP tab -> Members tab -> Failover Associations -> failover_association check box, and then click the Edit icon.
2. The DHCP Failover Association editor contains the following tabs from which you can modify data:
   - **General:** In the Basic tab, modify the fields as described in Adding Failover Associations.
   - In the Advanced tab, complete the following to modify the port number you use for the failover association:
     - **Failover Port:** Click Override to enter a port number for the failover association. You can use any available port from 1 to 65535. The default is 647 for a new installation and 519 for an upgrade.
   - **Triggers:** Before editing the triggers and timers, ensure that you understand the ramifications of the changes. Improper configuration of the triggers can cause the failover association to fail. For information about the fields in the Basic tab, see Adding Failover Associations. The following are the triggers in the Advanced tab:
     - **Max Response Delay Before Failover(s):** Specifies how much time (in seconds) can elapse before a failover occurs when a failover peer does not receive any communication from its peer. This number should be small enough that the transient network failure does not leave the servers out of communication for a long time, but big enough that the servers are not constantly connecting and disconnecting. The default is 60 seconds.
     - **Max Number of Unacked Updates:** Specifies the number of "unacked" packets the server can send before a failover occurs. The default is 10 messages.
     - **Max Client Lead Time (s):** Specifies the length of time that a failover peer can renew a lease without contacting its peer. The larger the number, the longer it takes for the peer to recover IP addresses after moving to the PARTNER-DOWN state. The smaller the number, the more load your servers experience when they are not communicating. The default is 3600 seconds.
     - **Max Load Balancing Delay (s):** Specifies the cutoff after load balancing is disabled. The cutoff is based on the number of seconds since a client sent its first DHCPDISCOVER message. For instance, if one of the failover peers gets into a state where it is busy responding to failover messages but is not responding to other client requests, the other peer responds to the client requests when the clients retry. This does not cause a failover. The default is three seconds.
   - **Failover Settings:** This is valid for Microsoft Management only. Modify failover association settings. For information, see Configuring Failover Associations.

If you modify failover settings from secondary Microsoft server settings, the appliance does not update failover settings on NIOS for the following reasons:

- When DHCP synchronization is disabled for primary Microsoft server, you must enable DHCP synchronization for primary Microsoft server to reflect the settings on NIOS.
- The primary synchronization interval must be completed. For example, consider that you are modifying failover settings from secondary Microsoft server settings where the synchronization interval for primary server is five minutes, and the time interval for the secondary server is one minute. In this case, failover settings are updated on NIOS only after the primary server synchronization interval, which is five minutes.
- **Extensible Attributes:** Add and delete extensible attributes that are associated with a failover association. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.

Monioring Failover Associations

After you configure a failover association, the peers establish a TCP connection for communication. In a normal operational state, they send keepalive messages and database updates every time they grant a lease. However, there are times when the failover association experiences problems and goes into a state other than NORMAL. You can monitor the overall status of a failover association and the individual status of the peers to verify that the servers are operating and communicating properly.

Both peers in a failover association maintain the same DHCP fingerprinting state (enabled or disabled) even when one of the peers fails or becomes operational again. Note that both peers must be in the same Grid for the fingerprinting state to stay the same. For information about DHCP fingerprinting, see About DHCP Fingerprinting.

In this panel, you can also modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.

To monitor the failover association status:

1. From the Data Management tab, select the DHCP tab -> Members tab -> IPv4 Failover Associations section. Grid Manager displays the list of failover associations and their overall status.
2. To view detailed information about a failover association, select the failover_association check box, and then click the Show Status icon.
3. In the Failover Association Status dialog box, Grid Manager displays the overall status of the failover association and the status of both the primary and secondary servers.

The failover association can be in one of the following states:

- **OK** (green): The failover association is functioning properly.
- **DEGRADED** (yellow): The failover association is degraded when one of the peers is giving out limited addresses.
- **FAILURE** (red): The failover association is not functioning, may be because it is not completely configured. The peers are not assigning IP addresses.

For each peer, Grid Manager displays the hostname or IP address, the status, and event date. The peer can be in one of the following states:
1. STARTUP: The server is starting up.
2. NORMAL: The server is in a normal operational state in which it responds to its load balancing subset of DHCP clients.
3. PAUSED: This state allows a peer to inform the other peer that it is going out of service for a short period of time so the other peer can immediately transition to the COMMUNICATIONS-INTERRUPTED state and start providing DHCP service to DHCP clients.
4. COMMUNICATIONS-INTERRUPTED: The servers are not communicating with each other. Both servers provide DHCP service to DHCP clients from which they receive DHCP requests.
5. PARTNER-DOWN: The server assumes control of the DHCP service because its peer is out of service.
6. RECOVER: The server is starting up and trying to get a complete update from its peer and discovers that its peer is in the PARTNER-DOWN state.
7. RECOVER-WAIT: The server has got a complete update from its peer and is waiting for MCLT period to pass before transitioning to the RECOVER-DONE state.
8. RECOVER-DONE: The server completed an update from its peer.
9. POTENTIAL-CONFLICT: The peers are not synchronized due to an administrative error or an incorrect state transition. Check the failover configuration and correct the error.
10. CONFLICT-DONE: This is a temporary state that the primary server enters after it received updates from the secondary server when it was in the POTENTIAL-CONFLICT state.
11. RESOLUTION-INTERRUPTED: The server responds to DHCP clients in a limited way when it is in this state.
12. UNKNOWN: The DHCP server is in an unknown state. The failover association is not functioning properly, may be because it is configured improperly. For example, failover association is not assigned to any DHCP range.
13. SHUTDOWN: This state allows a peer to inform the other peer that it is going out of service for a long period of time so the other peer can immediately transition to the PARTNER-DOWN state and completely assume control of the DHCP service.

**Note:** NIOS does not support PARTNER-DOWN and Force Recovery for a Microsoft DHCP failover association.

### Deleting Failover Associations

You cannot delete a failover association if it is currently assigned to a DHCP range. If you want to delete a failover association, ensure that it is not assigned to any DHCP range.

To delete a failover association:

1. From the Data Management tab, select the DHCP tab -> Members tab -> Failover Associations -> failover_association check box, and then click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes.

The appliance puts the failover association in the recycle bin, if enabled.

### Setting a Peer in the Partner-Down State

If one of the peers in a failover association is out of service for an extended period of time, you should consider putting the functional peer in the PARTNER-DOWN state. When you place the functional peer in the PARTNER-DOWN state, it assumes full DHCP services for the networks. Since the functional server may not receive all the updates from its peer, it extends all the leases on the MCLT. Once the following conditions are met, the functional peer provides DHCP services autonomously:

- It has reclaimed all the leases that belonged to its peer.
- The MCLT has passed.

When the peer that is offline comes back online, it synchronizes with the functional peer and reestablishes the communication before it provides DHCP services to the clients.

**WARNING:** Before you put a peer in the partner-down state, ensure that the other peer is indeed out of service. If both the primary and secondary servers are operational when you place one of them in the partner-down mode, both servers may stop issuing leases for a minimum of time defined in the MCLT.

To set a peer in the PARTNER-DOWN state:

1. From the Data Management tab, select the DHCP tab -> Members tab -> Failover Associations -> failover_association check box.
2. Expand the Toolbar and click Set Partner Down.
3. In the Set Failover Association Partner Down dialog box, select one of the following:
   - **Primary**: Select this if the secondary server is out of service.
   - **Secondary**: Select this if the primary server is out of service.
4. Click OK.

**Note:** You cannot place the functional peer in the PARTNER-DOWN state for a Microsoft DHCP failover in NIOS.
Performing a Force Recovery

When the primary and secondary peers are not synchronized, you can perform a force recovery to set the primary server in the PARTNER-DOWN state while putting the secondary server in the RECOVER state. During a force recovery, all leases in the databases are resynchronized. When you perform a force recovery, the secondary server does not serve any DHCP leases for a minimum of the MCLT while it resynchronizes with the primary server. Before you perform a force recovery, consult with Infoblox Technical Support or your Infoblox representative to ensure that the force recovery is appropriate for the situation.

To perform a force recovery:

1. From the Data Management tab, select the DHCP tab -> Members tab -> Failover Associations -> failover_association check box.
2. Expand the Toolbar and click Force Recovery State.
3. In the Force Secondary Peer Recovery State dialog box, click OK.

The appliance synchronizes the databases on the primary and secondary servers.

Note: You cannot place the functional peer in the PARTNER-DOWN state for a force recovery in NIOS.

Recovering DHCP Failover Associations

During a conflict resolution, when the primary peer of the DHCP failover association is in the CONFLICT-DONE state and the secondary peer in the POTENTIAL-CONFLICT state, the secondary peer might experience problems (such as restarting, network outage, etc.) and goes into an invalid state. This results in a deadlock state for the failover association, causing a DHCP service outage. When the failover association is in a deadlock state, you can perform a recovery for the failover association. You can run the recovery for one failover association at a time and when the primary member is in the CONFLICT-DONE state. This feature is supported for Infoblox appliances only and not for any other external DHCP servers.

Note: When the failover recovery is in progress, the DHCP service on both peers are disabled and you cannot enable the DHCP service until the failover recovery is successfully completed. You can view the logs of the failover recovery process in the syslog and infoblox.log file.

To recover a DHCP failover association:

1. From the Data Management tab, select the DHCP tab -> Members tab -> Failover Associations -> failover_association check box.
2. Expand the Toolbar and click Recovery from Deadlock State.
3. In the Failover Recovery Progress dialog box, click Start to start the recovery of the failover association from the deadlock state.
4. In the confirmation dialog box, click Yes.

Note: After you start the failover recovery, you cannot revert the changes.

Grid Manager starts the failover recovery and you can view the following information in the Failover Recovery Progress dialog box:

- **Failover association**: The name of the failover association.
- **Primary**: The hostname or IP address of the primary server.
- **Secondary**: The hostname or IP address of the secondary server.
- **Number of leases to be processed**: The total number of leases to be processed.
- **Number of leases processed**: The number of leases that have been processed.
- **Current Status**: Displays the current status of the failover recovery process. The current status can be one of the following:
  - **Pending**: The failover recovery is initiated for a failover association and the recovery process will start soon.
  - **Calculating**: The appliance calculates the total amount of leases to be processed.
  - **Applying**: The appliance looks for conflicts and tries to resolve the conflicts.
  - **Completed**: The failover recovery is completed successfully.
  - **Failed**: The failover recovery fails.

Grid Manager also displays the reason for the failure if that happens.

After successful completion of the failover recovery, you must restart both the primary and secondary peers to bring them back to the CONFLICT-DONE state.

You can stop the failover recovery operation by clicking Stop in the Failover Recovery Progress dialog box before the recovery process is complete.

Note: If for any reasons the recovery is blocked when the operation is in progress, you can cancel the current operation and start the recovery for the failover association again.

Chapter 31 Configuring IPv4 DHCP Filters

This chapter explains how to configure IPv4 DHCP filters. It contains the following sections:
About IPv4 DHCP Filters

To control how the appliance allocates IPv4 addresses, you can define DHCP filters and apply them to Grid, members, DHCP ranges, range templates, IPv4 network containers, IPv4 networks, shared networks, IPv4 network templates, IPv4 fixed addresses, IPv4 fixed address templates, IPv4 reservations, IPv4 reservation templates, and IPv4 host addresses. You can override filters set at an upper level and apply a new logic filter. Depending on your configuration, DHCP filters screen requesting clients by matching MAC addresses, relay agent identifiers, DHCP options, or DHCP fingerprints you define in the filters. If you configure DHCP servers in the Grid to send authentication requests to a RADIUS authentication server group, you can also filter requests by matching the authentication results. (For information about this feature, see Chapter 32, Authenticated DHCP.)

When you define DHCP filters, you classify DHCP clients based on the information provided by the clients or by the RADIUS server. When you apply filters to an address range, the appliance responds to your address requests based on your configuration. The appliance also decides which DHCP options to return to the matching clients based on how you apply the filters. For more information, see Applying Filters to DHCP Objects.

You can use filters to control address allocation based on your network requirements. For example, you can use DHCP filters to screen unmanaged hosts on a network by denying their address and option requests. If you have multiple DHCP address ranges on the same network and you want to assign IP addresses from specific address ranges to specific clients, you can use filters to screen the address assignments. For information, see IP Address Allocation.

The appliance supports the following filters:

- MAC address filters: Use MAC addresses as matching criteria for granting or denying address requests. For information, see About MAC Address Filters.
- Relay agent filters: Identify remote hosts by matching the relay agent identifiers in the DHCPDISCOVER messages. For information, see About Relay Agent Filters.
- Option filters: Classify hosts by matching the DHCP options and values sent by the requesting hosts. For information, see About Option Filters.
- DHCP fingerprint filter: Identify remote clients by matching the option number sequence or vendor ID sent in option 55 and 60 of the DHCP request against the DHCP fingerprints cached on the system. For information about DHCP fingerprint filters, see About DHCP Fingerprint Filters. For information about DHCP fingerprint detection, see DHCP Fingerprint Detection.
- NAC filters: Use authentication results from a RADIUS authentication server group as matching criteria for granting or denying address requests. For information, see Chapter 32, Authenticated DHCP.

You can use MAC, option, and NAC filters to define DHCP options that matching clients can receive. Depending on how you apply a filter, all DHCP clients with matching criteria can receive all or some of the DHCP options defined in the filter. DHCP options defined for a matching filter supersede those defined at the Grid, member, network, and DHCP range levels. Options defined for a filter that is in the Class Filter List of an address range supersede those defined in the Logic Filter List. For more information about how the appliance returns options and how to apply DHCP filters, see Applying Filters to DHCP Objects.

IP Address Allocation

When a DHCP client requests an IP address, the NIOS appliance draws an address from an address range associated with the network segment for that client. Because you define that range, you can thereby control the IP address (within the defined range) and the associated TCP/IP settings that the client receives.

In Figure 31.1, three hosts — each in a different subnet — request an IP address. Each one broadcasts a DHCPDISCOVER message, which includes its MAC address. When the router, which also functions as a DHCP relay agent, receives the message, it adds the IP address of the interface on which the message arrives and forwards the message to the DHCP server — or servers — previously configured on the router. When the NIOS appliance receives the message, it uses the ingress interface IP address of the router to determine the network segment to which the host belongs and associates the MAC address of the requesting host with an IP address from an address range for that network.
When each host broadcasts a DHCPDISCOVER message, it includes its MAC address.

When the relay agent receives the DHCPDISCOVER message, it adds the IP address of the ingress interface to the message, then forwards the message using IP unicast to the DHCP server.

When the NIOS appliance receives the DHCPDISCOVER message, it uses the ingress interface IP address on the relay agent to determine the network segment to which the host belongs. It then assigns an address to that host from the address range belonging to that subnet. Furthermore, it associates the IP address with the source MAC address of the host.

The NIOS appliance replies to DHCPREQUEST messages by sending DHCPOFFER messages through the relay agent to the requesting hosts, as shown in Figure 31.2.
The addressing scheme depicted in Figure 31.1 and Figure 31.2 is fairly simple: each network has a single address range. Consequently, address assignments are fairly straightforward. However, if you have multiple address ranges in the same network and you want to assign addresses from specific address ranges to specific hosts, you must screen the address assignments through the use of filters. If you do not apply a filter, the NIOS appliance assigns addresses from the highest address range to the lowest range and within each range from the highest address to the lowest address. That is, the appliance chooses the range with the highest addresses first (that is, closest to 255) and begins assigning addresses exclusively from that range, starting with the highest address and finishing with the lowest (closest to 0). When all the addresses from that range are in use, it then begins assigning addresses from the next highest range, and so on, finishing with the range with the lowest addresses. This is shown in Figure 31.3.

Note: After the DHCP server runs for a while, it assigns leases based on when it last used addresses, and not just on their positions in the range.

Figure 31.3 Multiple Address Ranges without Filters
IP Address Allocation Using Filters

To control the assignment of addresses from specific address ranges to specific hosts, the NIOS appliance provides the following filters:

- A MAC address filter to which you add MAC addresses as filter criteria. For information, see About MAC Address Filters.
- A relay agent filter with configured circuit ID and remote ID as specified by the relay agent (DHCP option 82). For information, see About Relay Agent Filters.
- An option filter in which you specify DHCP options and matching values. For information, see About Option Filters.
- A NAC filter in which you specify authentication results from a RADIUS authentication server group as filter criteria. For information, see About NAC Filters.

When the appliance receives an address request, it checks if the request matches a filter. If it does not, the appliance assigns an address from the address range with the highest available IP address. If the request matches at least one class filter for a range, the appliance applies the following rules:

- If there are grant address filters applied to that range, the request must match one of the class filters or the appliance does not grant an address from that range.
- If there are deny address filters applied to that range, the request must not match any of the filters. If the request matches a deny filter, the appliance does not grant an address from that range.
- If an address range has a combination of grant and deny filters, the request must:
  - Match a grant filter
  - Not match a deny filter

Two rules govern the behavior of the appliance in relation to DHCP filters:

1. Depending on your filter configuration, the appliance checks if any data in an address request (such as the MAC address of the client, DHCP options 77 and 82, etc.) matches any filters applied to an address range.
2. The appliance checks for available addresses in the address ranges containing the highest addresses first. ("Highest" means closest to 255.255.255.255, and "lowest" means closest to 0.0.0.0.)

These two rules can work in coordination. For example, when the appliance receives an address request, it first checks if the request matches any filter. If it matches more than one filter assigned to different address ranges, the appliance first applies the filter that belongs to the range with the highest IP addresses. If that address does not grant an address lease (because the filter action is Deny or all address leases in that range are already in use), the appliance then applies the matching filter for the range with the next higher set of IP addresses. If the appliance still has not granted a lease from the address ranges whose filters match data in the request and there are unfiltered address ranges, the appliance attempts to assign an address from one of these ranges, again beginning with the range having the highest IP addresses. Figure 31.4 presents an example illustrating the sequence in which the appliance assigns addresses when a request matches a MAC address filter. For information about MAC address filters, see About MAC Address Filters.

Figure 31.4 DHCP Address Assignment with Multiple Filters
if then
the appliance receives a request that matches a filter for one address range, it applies the action specified in the filter for that address range. If it does not assign an address from that range (the action is deny or the action is grant but all addresses in that range are in use), the appliance then checks if it can assign an address from an unfiltered address range (if there are any), starting with the range with the highest addresses first, as shown in Figure 31.3.

the same filter applies to multiple address ranges and the appliance receives an address request matching that filter, it checks the address range with the highest IP addresses matching that filter. If the appliance does not assign an address from that range, it checks the filtered address range with the next highest IP addresses, and so on. If it still has not assigned an address, the appliance starts checking unfiltered address ranges (if there are any), again beginning with the range with the highest address first.

multiple filters for the same address range conflict with each other (one filter grants a lease and another denies it) and a requesting client matches both filters, the filter denying the lease takes precedence. For example, if a requesting client matches both a MAC address filter (granting a lease) and a user class filter (denying a lease) for the same address range, the appliance denies the lease. When faced with a choice to either allow or deny a lease based on equal but contradictory filters, the appliance takes the more secure stance of denying it.

About MAC Address Filters

The appliance can filter an address request by the MAC address of a requesting host. Depending on how you apply the MAC filter, the appliance can grant or deny the address request if the requesting host matches the filter criteria. You can also define DHCP options that you want to return to the matching client if the options are so configured. The client can also request specific options to be returned through DHCP option 55. The appliance returns DHCP options to matching clients based on how you apply the filters. For information, see Applying Filters to DHCP Objects.

You can configure a MAC address filter or specific MAC addresses within a filter to expire after a certain amount of time has passed. Filter expiration is useful in situations where you want to keep filters running against updated MAC addresses. The permission to use the MAC addresses assigned to an IP address may become invalid after a certain period of time. For example, you can use a MAC address filter to restrict the right to use MAC addresses assigned to IP addresses for visiting guests or temporary workers. You can avoid removing invalid addresses from address filters manually by configuring the appliance to expire filters or to expire specific addresses within filters.

To apply a MAC address filter to an address range:

1. Define a MAC address filter. For information, see Defining MAC Address Filters.
2. Add a MAC address to the filter. For information, see Adding MAC Address Filter Items.
3. Apply the filter to a DHCP address range or range template, and specify that if the MAC address of a requesting host matches the filter definition, the appliance either grants or denies the address assignment. For information, see Applying Filters to DHCP Objects.

Defining MAC Address Filters
To define a MAC address filter:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 MAC Address Filter.

   or

   From any panel in the DHCP tab, expand the Toolbar and click Add -> IPv4 MAC Address Filter.

2. In the Add IPv4 MAC Filter wizard, complete the following:
   - Name: Enter a meaningful name for the filter. For example, if you want to filter address requests by department, you can name one filter "Marketing", another "Finance", and so on. The name must be unique within a specific network. If you want to specify option settings in the filter, the filter name must be unique among all MAC filters.
   - Comment: Enter useful information about the filter.

3. Click Next and complete the following to define the DHCP options to return to the matching client:
   - Option Space: Select an option space from the drop-down list. This field is displayed only when you have custom option spaces. The appliance uses the DHCP option space as the default.
   - Lease Time: Enter the value of the lease time in the field and select the time unit from the drop-down list.
   - The lease time applies to hosts that meet the filter criteria.

Options to Merge with Object Options
Click the Add icon. Grid Manager adds a new row to the table with the default DHCP option space and option name displayed. Complete the following:

- Option Space: Click the down arrow and select an option space from the drop-down list. The selected option space contains the corresponding DHCP options.
- Option Name: Click the down arrow and from the drop-down list, select the DHCP option you want to return to the requesting host.
- Value: Enter the value that you want the filter to return for the selected DHCP option. For example, enter the value 255.255.255.0 for the subnet-mask option.

To add more options to the filter, click the Add icon and repeat the steps.

4. Click Next and complete the following to configure the expiration setting:
   - Default MAC Address Expiration
   - Select one of the following to configure the expiration setting for the filter:
     - Never Expires: Select this if you want the MAC address filter to never expire. This is selected by default.
     - Automatically Expires in: Select this if you want the filter to expire after a specific time frame. You can specify the time in seconds, minutes, hours, or days. The filter expiration time you configure here affects how long the DHCP server grants a lease to a client. It has an upper limit of 15 minutes on the lease time you configure for the Grid. For example, if both the filter expiration time and the lease time are less than 15 minutes, the appliance uses the lease time. If both filter expiration time and lease time are greater than 15 minutes, the appliance uses the filter expiration time. If the filter expiration time is less than 15 minutes and the lease time is greater than 15 minutes, the DHCP server grants a lease for 15 minutes. If the filter expiration time is greater than 15 minutes and the lease time is less than 15 minutes, the appliance uses the lease time.
   - Enforce Expiration Times: Select this to enable the expiration setting.
   - Enabled: The filter is enabled by default. Clear the check box to disable this filter.

5. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes.

6. Save the configuration and click Restart if it appears at the top of the screen.

Adding MAC Address Filter Items

To add a MAC address to a MAC address filter:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 MAC Address Filter Item.

   or

   From any panel in the DHCP tab, expand the Toolbar and click Add -> IPv4 MAC Address Filter Item.

2. In the Add IPv4 MAC Address Filter Item wizard, complete the following:
   - MAC Address: Enter the MAC address in one of the following formats: aa:bb:cc:dd:ee:ff, aa-bb-cc-dd-ee-ff, aabbcc-dddef, and aabbccddeeff. The appliance displays the address in the AA:BB:CC:DD:EE:FF format. You can also enter a vendor prefix in the three hexadecimal format using the same separators supported in the MAC address format. For example, you can enter aa.bb.cc as the vendor prefix. The appliance displays AA:BB:CC.
   - Comment: Enter useful information about the filter item.
   - Expiration Time: MAC addresses in a filter stay valid until you explicitly configure them to expire. You can enable expiration for specific MAC addresses in the filter. Select one of the following:
     - Never Expires: Select this if you want the MAC address to never expire. This is selected by default.
Expires on: Select this and specify the Date and Time for the expiration. The fields display the current date and time. If you have already configured an expiration time for the filter, the appliance displays the time here by adding the filter expiration time to the current time. For example, if the expiration time for the filter is two days and the current date is June 6, 2009, the appliance displays June 8, 2009 in the Date field.

3. Click Next and select one of the following to configure user registration (optional):
- Register as User: Select this and enter a username in the field.
- Register as Guest: Select this and enter the first name, middle name, last name, email address, and phone number of the guest user.

The appliance displays the information you enter here in the lease viewers.

4. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes.

5. Save the configuration and click Restart if it appears at the top of the screen.

After you define a MAC address filter and add MAC addresses to it, you can assign the filter to a DHCP range. The appliance filters IP address requests based on the filter criteria. For information, see Applying Filters to DHCP Objects.

About Relay Agent Filters

The NIOS appliance can filter an address request by the circuit ID and remote ID of a requesting host. The filter instructs the appliance either to grant or deny an address request if the requesting host matches the filter. For information about the DHCP relay agent option, see About the DHCP Relay Agent Option (Option 82).

Option 82 assists the agent in forwarding address assignments across the proper circuit. When a relay agent receives a DHCPDISCOVER message, it can add one or two agent IDs (circuit ID and remote ID) in the DHCP option 82 suboption fields to the message, as illustrated in Figure 31.5. If the agent ID strings match those defined in a relay agent filter applied to a DHCP address range, the appliance either assigns addresses from that range or denies the request based on the configured parameters.

Figure 31.5 Relay Agent Filtering
To apply a relay agent filter to an address range:

1. Define a relay agent filter. For information, see Defining Relay Agent Filters.
2. Apply the filter to a DHCP address range or range template, and specify that if the circuit ID or remote ID of a requesting host matches the filter definition, the appliance either grants or denies the address assignment. For information, see Applying Filters to DHCP Objects.
3. Define the access privileges of limited-access admin group for relay agent filters. For information, see Managing Administrators.

Defining Relay Agent Filters

To define a relay agent filter:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 Relay Agent Filter.
2. In the Add IPv4 Relay Agent Filter wizard, complete the following:
   - Name: Enter a meaningful name for the filter. For example, you can enter the IP address or the name of the router acting as the relay agent. The name must be unique within a specific network.
   - Comment: Enter useful information about the filter.
3. Click Next to define the relay agent ID type. If you apply both ID types, the relay agent must provide both identifiers when submitting a DHCP address request.

Select one of the following for both Circuit ID and Remote ID:

- Any: Select this and the filter matches any of the circuit identifiers for remote hosts. You cannot select this for both circuit ID and remote ID at the same time.
- Not Set: Select this and no circuit identifier is set for remote hosts.
- Matches Values: Select this and enter the circuit ID or remote ID in the field. You can enter the ID in hexadecimal format, such as 1f:cd, ab, or ef:23:56, or in string format, such as abcd or aa:gg. The appliance matches the value you enter here with the value sent by the DHCP client in counted octet sequence format. This field supports wildcard characters and regular expressions. You can also select to have an exact match or a substring match, as follows:
  - Exact Match: Select this to match the exact value sent by the DHCP client that contains the value you entered in the Matches Values field.
  - Substring: Select this to match a substring of the value sent by the DHCP client. Enter the Offset and Length values for the substring match, as follows:
    - Offset: Enter the number of characters at which the match value for the substring starts. Enter 0 to start at the beginning of the value, enter 1 for the second position, and so on. For example, when you enter 2 and have a substring value of AFTR, the appliance matches the value AFTR starting at the third character of the match value.
    - Length: Enter the length of the substring value. For example, if the match value is AFTR, the length is 4.
4. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes.
5. Save the configuration and click Restart if it appears at the top of the screen.

After you define a relay agent filter, you can assign it to a DHCP range. The appliance responds to address requests based on the filter criteria. For information, see Applying Filters to DHCP Objects.

About Option Filters

You can use option filters to classify DHCP clients and decide which DHCP options each group of clients can receive. By default, regardless of the networks in which the DHCP clients reside and whether an option filter is applied to a DHCP range or range template, all DHCP clients that match the filter criteria receive the DHCP options and values you define in the filter. You can change this configuration so the appliance does not use the filter to classify DHCP clients. For information about how to configure this, see Defining Option Filters.

You can add DHCP options and the Hardware Operator option to an option filter. (For information about the Hardware Operator option, see DHCP Hardware Operator.) Depending on whether the options you add to the filter are also defined at the Grid, member, network, and DHCP range levels, and whether you add the filter to the Class Filter List or Logic Filter List, the appliance either appends them to the existing options or overwrites the option values before returning them to the matching clients. For more information about how the appliance returns DHCP options, see Adding Filters to the Logic Filter List.

The appliance can filter an address request by the options (such as root-server-ip-address or user-class) of the requesting host. Depending on how you apply an option filter, the appliance can grant or deny an address request if the requesting host matches the filter criteria. You can also create complex match rules that use the AND and OR logic to further define the filter criteria. When you select match rules in Grid Manager, you can preview the rules before committing them to the filter. Grid Manager provides an expression builder that automatically builds the rules after you define them. For information, see Defining Option Filters.

To define an option filter and apply it to an address range:

1. Define an option filter based on either the predefined or custom DHCP options. For information, see Defining Option Filters.
2. Apply the filter to a DHCP address range or range template in the Class Filter List or Logic Filter List. For information, see Applying Filters to DHCP Objects.
After you define an option space and add options to it, you can set up option filters and define option values. For example, to handle two different client classes, you can define two option filters (vendor-class_1 and vendor-class_2) and send different option values to different clients based on the vendor-class-identifier options that you obtain from the clients.

**DHCP Hardware Operator**

You can define the Hardware Operator option and add it as a match rule to an option filter. This option enables the appliance to match the hardware type and MAC address of the DHCP client, which it derives from the hardware type, hlen (hardware length) and chaddr (client hardware address) fields of the client's DHCP Discover and Renew packets.

To add Hardware Operator to an option filter, fill in the fields as follows:

- In the first drop-down list, select Hardware Operator. Note that because it is not a DHCP Option, it does not have an actual option number.
- In the second drop-down list, select one of the following operators: equals, does not equal, substring equals and substring does not equal.
  - If the operator is substring equals or substring does not equal, specify the offset and length.
- In the text field, enter the string that represents the hardware type and MAC address to match. For example, the htype value is 1 for the Ethernet hardware type. The hardware types (hrd) are defined at [http://www.iana.org/assignments/arp-parameters/arp-parameters.xml#hardware-type-rules](http://www.iana.org/assignments/arp-parameters/arp-parameters.xml#hardware-type-rules).

This filter rule assumes that the values exist in the DHCP packets.

The following table provides examples of rules that include the Hardware Operator option. The entry in the first drop-down list for all rules is **Hardware Operator**.

<table>
<thead>
<tr>
<th>Rule Description</th>
<th>Second Drop-Down List (operator)</th>
<th>Text Field (string)</th>
<th>Offset</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match a hardware type and MAC address.</td>
<td>equals</td>
<td>01:00:C0:00:AA:BB:CC</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Match hardware type only.</td>
<td>substring equals</td>
<td>01</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Match the vendor MAC prefix (first three bytes of MAC address).</td>
<td>substring equals</td>
<td>00:00:00:00:00:00</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

### Defining Option Filters

To define an option filter:

1. From the **Data Management** tab, select the **DHCP tab -> IPv4 Filters** tab, and then expand the Toolbar and click **Add -> IPv4 Option Filter**.
2. or
   - From any panel in the **DHCP tab**, expand the Toolbar and click **Add -> IPv4 Option Filter**.
3. In the **Add IPv4 Option Filter wizard**, complete the following:
   - **Name**: Enter a meaningful name for the option filter. For example, you can enter Linux if you plan to use this option filter to screen Linux systems. The name must be unique within a specific network. If you want to specify option settings in the filter, the filter name must be unique among all option filters.
   - **Comment**: Enter useful information about the filter.
   - **Apply this filter as a global DHCP class**: This check box is selected by default. When you select this check box, the appliance defines a global class statement in the dhcpd configuration file for members that have DHCP enabled, regardless of whether the filter is applied to a DHCP range or range template. All DHCP clients that belong to this class receive the DHCP options and values you define in the filter. When you clear this check box, you cannot apply this filter to the Class Filter List of a range or range template. You cannot clear this check box if the filter is currently applied to a range or range template. The appliance displays an error message when you try to save this configuration.
4. Click **Next** and complete the following to add match rules:
   - In the first drop-down list, select a DHCP option. For example, select user-class(77) for a specific user class, such as mobile users.
   - In the second drop-down list, select an operator.
     - If you select equals or does not equal, enter the value of the selected option you want the filter to match in the field.
     - If your operator and match value include a substring of an option value, enter the offset and length of the substring based on the following definitions:
       - **Offset**: Enter the number of characters at which the match value substring starts in the option data. Enter 0 to start at the beginning of the option data, enter 1 for the second position, and so on. For example, when you enter 2 and have a match value of MSFT, the appliance matches the value MSFT starting at the third character of the option data.
       - **Length**: Enter the length of the match value. For example, if the match value is MSFT, the length is 4.
You can do the following and repeat the filter selection steps to add another rule:

- Click » to add another rule at the same level.
- Click [ ] to add an all (logical AND) or any (logical OR) operator line and a parenthetical rule that is indented one level and above the first rule.
- Click [ ] to add an all (logical AND) or any (logical OR) operator line and a parenthetical rule that is indented one level.

After you add all the match rules, you can click Preview to view the rules that are written to the dhcpd configuration file or click Reset to remove the previously configured rules and start again. For information about how to use match rules, see bookmark2522.

4. Click Next and complete the following to define which DHCP options to return to the matching client:

- Option Space: Select an option space from the drop-down list. This field is not displayed if you do not have custom option spaces. The appliance uses the DHCP option space as the default.
- Lease Time: Enter the value of the lease time in the field and select the time unit from the drop-down list. The lease time applies to hosts that meet the filter criteria.

Options to Merge with Object Options
Click the Add icon. Grid Manager adds a new row to the table with the default DHCP option space and option name displayed. Complete the following:

- Option Space: Click the down arrow and select an option space from the drop-down list. The selected option space contains the corresponding DHCP options that you can use as filter criteria.
- Option Name: Click the down arrow and from the drop-down list, select the DHCP option you want to use as filter criteria.
- Value: Enter the match value that you want the filter to use for the selected DHCP option. To add more options to the filter, click the Add icon and repeat the steps.

5. Click Next to define extensible attributes. For information, see Using Extensible Attributes.

6. Save the configuration and click Restart if it appears at the top of the screen.

Using Match Rules in Option Filters
Each match rule you define in an option filter further defines the filter criteria of a matching client. You can add multiple match rules to an option filter. The appliance writes these rules to the dhcpd configuration file. You can also create complex match rules that use the AND and OR logic to further define the filter criteria. After you define the match rules, you can preview the rules before committing them to the filters.

For example, you can define the following rules in an option filter:

```
DHCP option = vendor-class-identifier
Substring offset = 0 (the match value starts at the beginning of the option data received from the client)
Substring length = 4 (the length of the match value MSFT)
Match value = MSFT
```

The appliance generates the following rules in the dhcpd configuration file:

```c
class "microsoft-other" {
    match if substring (option vendor-class-identifier,
        0, 4) = "MSFT";
    vendor-option-space MSFT;
}
```

You can also define more complex rules using the AND and OR logic as follows:

```
DHCP option = vendor-class-identifier
Match value = infoblox2000a
OR
```
DHCP option = vendor-encapsulated-options
Substring offset = 0 (the match value starts at the first character of the option data received from the client)
Substring length = 8 (the length of the match value infoblox)
Match value = infoblox
AND
DHCP option = vendor-encapsulated-options
Substring offset = 10 (the match value starts at the ninth character of the option data received from the client)
Substring length = 5, the length of the match value 2000a
Match value = 2000a

The appliance generates the following rules in the dhcpd configuration file:

class "infoblox" {
  match if (option vendor-class-identifier=infoblox2000a:) or
    ((substring(option vendor-encapsulated-options,0,8)="infoblox") and
     (substring(option vendor-encapsulated-options,10,5)="2000a"));
  vendor-option-space DHCP
}

Configuring User Class Filters

The NIOS appliance can filter DHCP address requests by user class filters. A user class indicates a category of user, application, or device of which the DHCP client is a member. User class identifiers are configured on DHCP clients and are sent during a DHCP address request operation. The client includes the user class identifier in DHCP option 77 when sending DHCPDISCOVER and DHCPREQUEST messages.

By using user class identifiers, a DHCP server can screen address requests and assign addresses from select address ranges based on the different user class identifiers it receives. For example, if you assign a user class filter named mobile to a range of addresses from 10.1.1.31–10.1.1.80, the appliance selects an address from that range if it receives an address request that includes the user class name mobile and there are still addresses available in that range. You might want mobile users to receive these addresses because you have given them shorter lease times than other, more stationary DHCP clients. See Figure 31.6.

Figure 31.6 Applying User Class Filtering

The user class for laptop A is mobile. When it sends DHCPDISCOVER and DHCPREQUEST messages, it includes its user class in the DHCP option 77 field.

The NIOS appliance has a filter that screens address requests by user class. If the user class for a DHCP client is mobile, the appliance assigns it an address from address range 2.

Note: The leases for addresses in address range 2 are shorter than those for more stationary computers. The intended use for address range 2 is to provide IP addresses for mobile users who log in to the network for relatively short periods of time and, therefore, do not require longer leases.
If the NIOS appliance receives address requests with the user class mobile and there are no available addresses in address range 2 but there are available addresses in ranges 1 and 3, the appliance begins assigning addresses from address range 3 (because its addresses are higher than those in range 1). Then, if all addresses in range 3 are in use, the appliance begins assigning addresses from address range 1. If you want the appliance to assign addresses to mobile users (that is, those identified with the user class mobile) exclusively from address range 2, then you must apply user class filters for “mobile” to address ranges 1 and 3 that deny lease requests matching that user class.

Configuration Example: Using Option Filters

The following example shows you how to create an option space, add custom options to it, create an option filter, and a match rule to filter the options so that the NIOS appliance can filter an address request by the vendor options of the requesting hosts. It can grant or deny an address request if the requesting host matches the filter.

1. Add an option space called MSFT, and then add the following options to it. For information, see Applying DHCP Options.

<table>
<thead>
<tr>
<th>Option name</th>
<th>Code</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>root-mount-options</td>
<td>1</td>
<td>Text</td>
</tr>
<tr>
<td>root-server-ip-address</td>
<td>2</td>
<td>IP address</td>
</tr>
<tr>
<td>root-server-host-name</td>
<td>3</td>
<td>Text</td>
</tr>
<tr>
<td>root-server-path-name</td>
<td>4</td>
<td>Text</td>
</tr>
<tr>
<td>swap-server-ip-address</td>
<td>5</td>
<td>IP address</td>
</tr>
<tr>
<td>swap-file-path-name</td>
<td>6</td>
<td>Text</td>
</tr>
<tr>
<td>boot-file-path-name</td>
<td>7</td>
<td>Text</td>
</tr>
<tr>
<td>posix-timezone-string</td>
<td>8</td>
<td>String</td>
</tr>
<tr>
<td>boot-read-size</td>
<td>9</td>
<td>16-Bit unsigned integer</td>
</tr>
</tbody>
</table>

2. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab and click the Add icon.

3. In the Add IPv4 Filter wizard, enter the filter name i86pc, and then select Options as the filter type.

4. Select MSFT as the option space, select an option, specify a value for it, and then add it to the i86pc option filter. You can select multiple options. Add the following options to the i86pc option filter:

<table>
<thead>
<tr>
<th>Option name</th>
<th>Code</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>root-server-ip-address</td>
<td>2</td>
<td>IP address</td>
</tr>
<tr>
<td>root-server-host-name</td>
<td>3</td>
<td>Text</td>
</tr>
<tr>
<td>root-server-path-name</td>
<td>4</td>
<td>Text</td>
</tr>
<tr>
<td>boot-file-path-name</td>
<td>7</td>
<td>Text</td>
</tr>
</tbody>
</table>

5. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab -> filter_name, and then click the Add icon.

6. In the Add IPv4 Match Rule wizard, select i86pc as the option filter, select vendor-class-identifier(60) as the matching option, and then enter MSFT as the matching value.

7. Add a DHCP range to the network. For information, see Configuring IPv4 Address Ranges.

8. Apply the i86pc option filter to the DHCP address range. For information, see Applying Filters to DHCP Objects.

9. Click Restart to restart services.

About DHCP Fingerprint Filters

The appliance can filter an address request by the DHCP fingerprint of a requesting client. Depending on how you apply DHCP fingerprint filters, the appliance can grant or deny the address request if the requesting client matches the filter criteria. Note that only superusers can add, modify, and delete DHCP fingerprint filters. Limited-access users cannot perform any DHCP fingerprint filter related tasks, though with the correct permissions they can apply DHCP fingerprint filters to DHCP ranges and range templates. For information about how to apply filters to DHCP ranges, see Applying Filters to DHCP Objects.

You can define a DHCP fingerprint filter by selecting one or multiple DHCP fingerprints from the existing list of DHCP fingerprints, and then assign a grant or deny permission to the filter. You can then apply the filter to a DHCP address range, if DHCP fingerprint detection is enabled.
To define a DHCP fingerprint filter:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 Fingerprint Filter.
   From any panel in the DHCP tab, expand the Toolbar and click Add -> IPv4 Fingerprint Filter.
2. In the Add IPv4 Fingerprint Filter wizard, complete the following:
   - Name: Enter a meaningful name for the filter. For example, if you want to filter address requests by a specific device class, you can name one filter "Gaming Console," another "Android Phones," and so on. The filter name must be unique among all DHCP fingerprint filters.
   - Comment: Enter useful information about the filter.
3. Click Next and then click the Add icon in the Select Fingerprints table. In the Fingerprint Selector dialog box, select the DHCP fingerprint you want to include in this filter. Click Add icon to select another DHCP fingerprint.

Note: When you select No Match, the appliance applies the filter to all requesting clients that do not send option 55 and option 60 or to clients that send values in option 55 and 60 that do not match any existing DHCP fingerprints.

4. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes.
5. Save the configuration.

Applying Filters to DHCP Objects

To further control how the appliance allocates IPv4 addresses to DHCP client requests, you can apply DHCP filters to determine the following:

- The class statements
- The address ranges from which it assigns leases
- When to grant or deny leases to the matching clients
- Which DHCP options to return to the matching clients

You can apply IPv4 logic filters at the Grid DHCP or Member DHCP. You can choose to keep the inherited properties or override them when you edit the IPv4 networks, IPv4 network containers, IPv4 network templates, IPv4 shared networks, IPv4 DHCP ranges, IPv4 DHCP range templates, IPv4 fixed addresses, IPv4 reservations, IPv4 fixed address templates, IPv4 reservation templates, or IPv4 host addresses.

Adding Filters to the Class Filter List

You can apply any DHCP filter to the Class Filter List of a DHCP range or range template. The appliance uses the matching rules of these filters to select the address range from which it assigns a lease. You can define permissions for these filters to instruct the appliance whether to grant or deny a lease to the matching client. When you add a filter with a grant permission, the client must match the filter criteria to receive a lease. When you define a filter with a deny permission, clients that do not match the filter criteria still receive leases. Only the client that matches the filter criteria is denied a lease.

Filters in the Class Filter List correspond to the class statement generated in the dhcpd configuration file, which is a classification of the client packet. All DHCP clients that match the option filter and relay agent filter criteria become members of the same class and are eligible to receive DHCP options for that class, regardless of the networks in which the clients reside. However, a client can only become a member of the MAC or NAC filter class when it is granted a lease from the DHCP range based on the filter criteria. Whether a client receives specific options and option values depends on the hierarchy of the options and how you apply the filters. For information about how the appliance returns DHCP options, see Adding Filters to the Logic Filter List.

Adding Filters to the Logic Filter List
The filters you add to the Logic Filter List correspond to the match rules that are written to the dhcpd configuration file. The appliance uses these filters to identify DHCP options and values to return to the matching clients. You can apply option, MAC, and NAC filters to the Logic Filter List. Note that a DHCP client is eligible to receive DHCP options defined in a filter if it matches the filter criteria. Whether the client receives specific options and their corresponding values depends on the hierarchy of the options and the list of options requested by the client through DHCP option 55. You can configure the appliance to ignore the option list requested by a matching client and return all the options that the client is eligible to receive. For information about how to ignore the option list requested by a client, see Configuring General IPv4 DHCP Properties.

**Note:** The appliance allows you to add an empty IPv4 logic filter at the end of the logic filter list, which means that you can add an IPv4 logic filter without defining DHCP options in it. In addition, you can change the order of the filters in the logic filter list.

The appliance decides which options and values to return to a client based on the following:

- If you have different DHCP options defined in a range and any DHCP filters in the Class Filter and Logic Filter lists, and these options do not overlap, the appliance merges and returns all options to the matching client. For example, a DHCP client obtains a lease from a DHCP address range (R) through an option filter in the Class Filter List (CF), which contains an option statement (O1) with a value of (S1). The appliance then matches a filter in the Logic Filter List (LF) that contains an option statement (O2) with a value of (S2). In this case, option statements O1 and O2 and their values S1 and S2 are merged and returned to the matching client.
- If there are overlapping DHCP options in a range and any DHCP filters in the Class Filter and Logic Filter lists, the values defined in the Class Filter List filters take precedence over those defined in the range and filters in the Logic Filter List. The appliance returns the option value defined in the class filters to the matching client. For example, a DHCP client obtains a lease from a DHCP address range (R) through an option filter in the Class Filter List (CF), which contains an option statement (O1) with a value of (S1). The appliance then matches a filter in the Logic Filter List (LF) that contains the same option statement (O1) with a value of (S2). In this case, the option value S1 defined in the option filter in the Class Filter List takes precedence and is returned to the DHCP client.
- When you apply option, MAC, and NAC filters to the Logic Filter List, the appliance translates their match rules into a DHCP if/elseif/else statement using the match rules of the first filter on the list as the "if" expression in the statement. Match rules in subsequent filters are translated into the "elseif" statements, and the last filter that does not contain any match rules is translated into the "else" statement. Note that a filter without any match rules can only be added as the last filter in the Logic Filter List.

For more information about how the appliance grants and denies leases to requesting clients and determines which DHCP options to return to the matching clients, see Configuration Example: Using the Class and Logic Filter Lists.

To apply IPv4 filters:

1. **Grid:** From the Data Management tab -> DHCP tab, select Grid DHCP Properties from the Toolbar.
   - **Member:** From the Data Management tab, select the DHCP tab -> Members tab -> member check box -> Edit icon.
   - **Network:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.
   - **DHCP Range:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.
   - **Fixed Address:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> fixed_address check box, and then click the Edit icon.
   - **IPv4 Reservation:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> reservation check box, and then click the Edit icon.
   - **Host Address:** From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> host_record check box, and then click the Edit icon.
   - **IPv4 Network or Fixed Address Template:** From the Data Management tab, select the DHCP tab -> Templates tab -> (IPv4 network or fixed address) template check box, and then click the Edit icon.
2. In the editor, click **Toggle Advanced Mode**, and then select the IPv4 Filters tab.
3. **Logic Filter List:** You can keep the inherited IPv4 logic filters or override them. To override the value that has been inherited from the upper level, click **Override**. Click the Add icon to add a filter to match a client based on the match rules defined in the filter. For more information, see Adding Filters to the Logic Filter List. If you have only one configured DHCP filter, the appliance displays the filter in the table. Otherwise, in the DHCP Filter Selector dialog box, click the filter you want to add. Use SHIFT+click and CTRL+click to select multiple filters.
4. Complete the following to add the Class Filter to a DHCP address range:
   - Click the Add icon to add a filter to identify the class of a matching client, and to grant or deny a lease to a client. For more information, see Adding Filters to the Class Filter List.

If you have only one configured DHCP filter, the appliance displays the filter in the table. Otherwise, in the DHCP Filter Selector dialog box, click the filter you want to add. Use SHIFT+click and CTRL+click to select multiple filters.

For each filter you add, click the **Action** column and select one of the following from the drop-down list:

- **Grant lease:**
  - For MAC address filters: Select this to assign an IP address from the address range to a requesting host whose MAC address matches the MAC address in the filter.
  - For relay agent filters: Select this to assign an IP address from the address range when one or both of the relay agent identifiers of the requesting host match the filter criteria.
  - For option filters: Select this to assign an IP address from the address range to a requesting host whose DHCP options match the DHCP options and match rules defined in the filter.
  - For NAC filters: Select this to assign an IP address from the address range to a requesting host based on the authentication results from a RADIUS authentication server group.
  - For DHCP fingerprint filters: Select this to grant a lease from the address range to a requesting host based whose DHCP fingerprint matches the DHCP fingerprint in the filter.
Deny lease:
For MAC address filters: Select this to deny an address request from a host whose MAC address matches a MAC address in the filter.
For relay agent filters: Select this to deny an address request when one or both relay agent identifiers match the filter criteria in the filter.
For option filters: Select this to deny an address request from a host whose DHCP options match the options and match rules in the filter.
For NAC filters: Select this to deny an address request from a host based on the authentication results from a RADIUS authentication server group.
For DHCP fingerprint filters: Select this to deny a lease request when the DHCP fingerprint of the requesting host matches the DHCP fingerprint in the filter.

The appliance uses filters in both the Class Filter and Logic Filter lists to determine the DHCP options and values it returns to the matching clients.

Note: You can only add a filter that does not contain any match rules as the last filter in the Logic Filter List.

5. Save the configuration and click Restart if it appears at the top of the screen.

Configuration Example: Using the Class and Logic Filter Lists

The following example shows you how to define DHCP filters and apply them to the class and logic filter lists. It also shows you the DHCP configuration file that is generated based on the configuration.

In this example, you first define a MAC filter, two option filters (one without match rules), and a NAC filter, and then apply the MAC filter to the Class Filter List and the other filters to the Logic Filter List of the address range 10.34.34.6 - 10.34.34.55.

1. Configure and save a MAC filter as follows. For more information, see Defining MAC Address Filters.
   a. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 MAC Address Filter.
   b. In the Add IPv4 MAC Filter wizard, complete the following:
      - Name: Enter MAC1.
   c. Click Next and complete the following to define the DHCP options to return to the matching client:
      - Lease Time: Enter 1234 and select seconds from the drop-down list.

      Options to Merge with Object Options: Click the Add icon. Grid Manager adds a new row to the table with the default DHCP option space and option name displayed. Complete the following:
      - Option Name: Click the down arrow and select log-server(7) from the drop-down list.
      - Value: Enter 10.34.34.3 as the value for the log-server option that is sent to the client in the OFFER/ACK message.

   d. Save the configuration.

2. Add a MAC address filter item as follows. For more information, see Adding MAC Address Filter Items.
   a. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 MAC Address Filter Item.
   b. In the Add IPv4 MAC Address Filter Item wizard, complete the following:
      - MAC Address Filter: Click Select Filter. In the DHCP Filter Selector dialog box, click MAC1.
      - MAC Address: Enter AB:DE:CC:DD:EE:01 as the MAC address.
   c. Save the configuration.

3. Configure and save an option filter with match rules as follows. For more information, see Defining Option Filters.
   a. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 OptionFilter.
   b. In the AddIPv4OptionFilter wizard, complete the following:
      - Name: Enter Option1.
   c. Click Next and complete the following to add match rules:
      - In the first drop-down list, select vendor-class-identifier.
      - In the second drop-down list, select substring equals, and then enter the following:
        - Offset: Enter 0 to match the value starting at the first character of the option data.
        - Length: Enter 4.
        - Enter MSFT as the matching value.

   d. Click Next and complete the following to define the DHCP options to return to the matching client:
Options to Merge with Object Options: Click the Add icon. Grid Manager adds a new row to the table with the default DHCP option space and option name displayed. Complete the following:

- **Option Name**: Click the down arrow and from the drop-down list, select `time-server(4)`.
- **Value**: Enter `10.34.34.2` as the value for the time-server option that is sent to the client in the OFFER/ACK message.

e. Save the configuration.

4. Configure and save another option filter without match rules as follows:

a. In the `AddIPv4OptionFilter` wizard, complete the following:
   - **Name**: Enter `Option2`.
b. Click **Next**. Do not define any match rules.
c. Click **Next** again and complete the following to define the DHCP options to return to the matching client:

   Options to Merge with Object Options: Click the Add icon. Grid Manager adds a new row to the table with the default DHCP option space and option name displayed. Complete the following:

   - **Option Name**: Click the down arrow and from the drop-down list, select `domain-name(8)`.

d. Save the configuration.

5. Configure and save a NAC filter as follows. For more information, see [Defining NAC Filters](#).

a. From the **Data Management** tab, select the **DHCP** tab -> **IPv4Filters** tab, and then expand the Toolbar and click **Add** -> **IPv4N ACFilter**.
b. In the **AddFilter Wizard**, complete the following and click **Next**:
   - **Name**: Enter `NAC1`.
c. Create a rule as follows:
   - In the first drop-down list, select `Compliance State`
   - In the second drop-down list, select `equals`
   - In the third drop-down list, select `Compliant`.

   Click **Preview** and the appliance displays the expression: `(Sophos.ComplianceState="Compliant")`.

d. Click **Next** and complete the following to define DHCP options:

   - **Lease Time**: Enter `1000` and select `seconds` from the drop-down list.

   Options to Merge with Object Options: Click the Add icon. Grid Manager adds a new row to the table with the default DHCP option space and option name displayed. Complete the following:

   - **Option Name**: Click the down arrow and from the drop-down list, select `cookies-servers(8)`.
   - **Value**: Enter `10.34.34.5`.

e. Save the configuration.

6. Apply the filters to the address range as follows. For more information, see [Applying Filters to DHCP Objects](#).

a. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> `10.34.34.6-10.34.34.55` check box, and then click the **Edit** icon.
b. In the **DHCP Range** editor, click **ToggleAdvancedMode**.
c. Click the **IPv4Filters** tab and complete the following:
   - **Class Filter List**: Click the Add icon and add `MAC1` as a class filter. Click the **Action** column and select **Grant lease** from the drop-down list.
   - **Logic Filter List**: Click the Add icon and add `Option1`, `NAC1`, and `Option2` respectively as logic filters.

d. Save the configuration.

The appliance generates the following information in the DHCP configuration file based on the filter configuration in this example:

```bash
# MAC filter "MAC1"

class "MAC1"  {
    default-lease-time 1234;
    min-lease-time 1234;
    max-lease-time 1234;
    option log-servers 10.34.34.3;
}

# NAC filter "NAC1"

{option sophos.compliance

```
state="compliant"
}
subnet 10.34.34.0 netmask 255.255.255.0 {
    pool {
        infoblox-range 10.34.34.6 10.34.34.55;
        range 10.34.34.6 10.34.34.55;
        option routers 10.34.34.1;
        # INFOBLOXMACFILTERDEBUGINFO: allow members of "MAC1";
        if (substring(option vendor-class-identifier,0,4)="MSFT") {
            # Option filter "Option1"
            option time-servers 10.34.34.2;
        }
        elsif (option Sophos.ComplianceState="Compliant") {
            # NAC filter "NAC1"
            default-lease-time 1000;
            min-lease-time 1000;
            max-lease-time 1000;
            option cookie-servers 10.34.34.5;
        }
        else {
            # Option filter "Option2"
            default-lease-time 2500;
            min-lease-time 2500;
            max-lease-time 2500;
            option domain-name "www.infoblox.com";
        }
    }
}

Depending on client requests and the matching criteria, the following scenarios can happen in this example:

If the requesting client matches the MAC1 and Option1 filters, the appliance returns the following:

- **Lease time = 1234 seconds** (from the MAC filter)
- **Returned options:**
  - Router(3) with a value of 10.34.34.1 (from the address range)
  - Log-server(7) with a value of 10.34.34.3 (from the MAC filter MAC1)
  - Time-server(4) with a value of 10.34.34.2 (from the option filter Option1)

If the requesting client matches the MAC1 and NAC1 filters, the appliance returns the following:

- **Lease time = 1234 seconds** (from the MAC filter MAC1)
- Returned options:
  - Router(3) with a value of 10.34.34.1 (from the address range)
  - Log-server(7) with a value of 10.34.34.3 (from the MAC filter MAC1)
  - Cookie-server(8) with a value of 10.34.34.5 (from the NAC filter NAC1)

If the client matches the MAC1 filter, but not the Option1 or NAC1 filters, the appliance returns the following:

- **Lease time = 1234 seconds** (from the MAC filter)
- **Returned options:**
  - Router(3) with a value of 10.34.34.1 (from the address range)
  - Log-server(7) with a value of 10.34.34.3 (from the MAC filter MAC1)
  - Domain-name(6) with a value of www.infoblox.com (from the option filter Option2)

If the requesting client does not match the MAC1 filter, no lease is granted.
Managing DHCP Filters

You can do the following to manage DHCP filters:

- Modify filter settings. For information, see Modifying DHCP Filters.
- View a complete list of filters, MAC address items, and match rules. For information, see Viewing DHCP Filters.
- Delete filters that are not in use. For information, see Deleting Filters.

Modifying DHCP Filters

To modify a filter:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab -> filter_name check box, and then click the Edit icon.
2. For a MAC address filter, the DHCP MAC Filter editor provides the following tabs from which you can modify information:
   - General: Modify the fields as described in Defining MAC Address Filters.
   - DHCP Options: Add or delete DHCP options. For information, see Defining MAC Address Filters.
   - Extensible Attributes: Add or delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.
   - Permissions: This tab appears only if you belong to a superuser admin group. For information, see About Administrative Permissions.

For a relay agent filter, the Relay Agent Filter editor provides the following tabs from which you can modify information:

- General: Modify the fields as described in Defining Relay Agent Filters.
- Extensible Attributes: Add and delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.

For an option filter, the Option Filter editor contains the following tabs from which you can modify information:

- General: Modify the fields as described in Defining Option Filters.
- Rules: Modify the match rules as described in Defining Option Filters.
- DHCP Options: Modify option spaces and DHCP options in the Basic tab as described in Defining Option Filters. You must define the PXELeaseTime in the Advanced tab.
- BOOTP: Modify BOOTP settings as described in Configuring IPv4 BOOTP and PXE Properties.
- Extensible Attributes: Add or delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.

For a DHCP fingerprint filter, the Add IPv4 Fingerprint Filter editor provides the following tabs from which you can modify information:

- General: Modify general information, such as the name and device class, as described in Defining DHCP Fingerprint Filters.
- Fingerprints: Add or delete DHCP fingerprints as described in Defining DHCP Fingerprint Filters.
- Extensible Attributes: Add and delete extensible attributes that are associated with the DHCP fingerprint filter. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.

For a NAC filter, the NAC Filter editor contains the following tabs from which you can modify information:

- General: Modify the name and comment.
- Rules: Modify the rules as described in Defining NAC Filters.
- DHCP Options: Add or delete DHCP options. For information, see Defining NAC Filters.
- Extensible Attributes: Add and delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.

3. Save the configuration and click Restart if it appears at the top of the screen.

You can modify the MAC address filter items and match rules for corresponding MAC address filters and option filters. For information, see 4823885 and 4823885.

Modifying MAC Address Filter Items

To modify a MAC address filter item:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab -> filter_name -> mac_filter check box, and then click the Edit icon.
2. The MAC Address Filter Item editor contains the following tabs from which you can edit data:
   - General: Modify the fields as described in Adding MAC Address Filter Items.
   - Registration: Modify registration settings as described in Adding MAC Address Filter Items.
   - Extensible Attributes: Add or delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.
3. Save the configuration and click Restart if it appears at the top of the screen.
Viewing DHCP Filters

To view DHCP filters:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab.
2. Grid Manager displays the following for each filter:
   - **Name**: The name of the filter.
   - **Filter Type**: The filter type.
   - **Comment**: The information about the filter.
   - **Site**: The location to which the filter belongs. This is one of the predefined extensible attributes.

Viewing MAC Address Filter Items

To view a list of MAC addresses in a specific MAC address filter:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab -> filter_name.
2. Grid Manager displays the following:
   - **MAC Address**: The DHCP fingerprint information of client's device. This field is displayed only when users use captive portal for authentication. MAC address assigned to the filter.
   - **Username**: Grid Manager displays the username to which the MAC address belongs in the lease viewers.
   - **Comment**: The information you entered about the filter item.
   - **Expiration Time**: The expiration time you configured for the MAC address.
   - **Fingerprint**: The DHCP fingerprint information of client's device. This field is updated when users use Captive Portal for authentication.
   - **Site**: The location to which the filter belongs. This is one of the predefined extensible attributes.

Deleting Filters

You can delete a filter that is not currently assigned to a DHCP range. You can also remove a filter from a DHCP range, and then delete the filter if it is not in use.

To delete a filter:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab -> filter_name, and then click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes.

The appliance puts the deleted filters in the Recycle Bin, if enabled. You can later restore the filter if needed.

To schedule this task, click the Delete icon -> Schedule Delete. In the Schedule Deletion dialog box, click Delete Later, and then specify a date, time, and time zone.

Chapter 32 Authenticated DHCP

This chapter includes the following sections:

- About Authenticated DHCP
  - DHCP Authentication Process
- Configuring DHCP Authentication
- About Authentication Server Groups
  - Configuring a RADIUS Authentication Server Group
  - Configuring an Active Directory Authentication Server Group
- About the Captive Portal
  - Configuring Captive Portal Properties
  - Customizing the Captive Portal Interface
  - Managing Captive Portal Certificates
  - Starting the Captive Portal Service
- Defining the IPv4 Network and DHCP Ranges
- Defining MAC Address Filters
- Using the Captive Portal Wizard
- Adding and Modifying the Filters and Associations
- Monitoring DHCP Authentication
- Viewing DHCP Ranges and Filters
- Configuration Example: Configuring Authenticated DHCP
- NAC Integration
- Configuring NAC with RADIUS Servers
- About Authentication Servers
  - Adding a Server Group
  - Associating a Server Group with a Member
  - Managing Server Groups
  - Clearing the Authentication Cache
- Configuring DHCP Ranges
About Authenticated DHCP

This feature provides the ability to control access to your IPv4 networks. (This feature does not support IPv6 networks.) You can divide a network into segments for unauthenticated, authenticated and guest users, and the DHCP server assigns clients to the appropriate segment based on their MAC addresses and authentication credentials.

For example, you can divide a network into one or more production segments for valid employees and systems, a guest segment with access only to the Internet and/or limited public servers, and a quarantine segment with access to a captive portal only. A captive portal is a web page that can provide an option to register as an authenticated user or as a guest.

On a member DHCP server, configure DHCP ranges for each access level — quarantine, authenticated, and guest — and create MAC address filters for the DHCP ranges. You can use DHCP options and Access Control Lists (ACLs) on your routers and firewall policies to define the appropriate services for each access level. On another Grid member, configure the captive portal and specify the authentication server group that authenticates the users. You can configure an authentication server group for external servers running RADIUS, LDAP, or Active Directory (AD).

When a DHCP client first sends a request for an IP address, the DHCP server offers an IP address from the quarantine range and directs the client to the captive portal, where the user can register either as an authenticated user or as a guest. When users sign in as guests or are successfully authenticated, the member automatically adds their MAC addresses to the appropriate MAC address filters and assigns addresses out of the appropriate address range.

DHCP Authentication Process

This section illustrates the DHCP authentication process. As illustrated in Figure 32.1, the DHCP authentication process begins when a DHCP client attempts to connect to the network. The member DHCP server checks if the MAC address of the DHCP client matches a MAC address in the guest or authenticated MAC address filters. If the member does not find a match, it assigns an IP address from the quarantine range to the DHCP client. When the client tries to access a web site, it is redirected to the captive portal page.

Note that the quarantine range in Figure 32.1 contains MAC address filters to deny leases in the quarantine range to DHCP clients with MAC addresses that match those in the Guest and Authenticated MAC address filters.

When the client connects to the captive portal IP address through its web browser, the user can register and continue the authentication process to obtain an IP address from the authenticated DHCP range, or register as a guest and obtain an IP address from the guest DHCP range. If the user chooses to continue the authentication process, as shown in Figure 32.2, the member authenticates the user with the authentication service that you configured, which can be RADIUS, LDAP, or AD.
After the client successfully passes the authentication stage, the appliance stores the MAC address of the client in the MAC address filter for the authenticated range. When the client tries to renew its IP address, it receives a new IP address from the authenticated DHCP range. Note that if the MAC address filter has an expiration period, the member automatically deletes expired MAC addresses from the filter. Therefore, if a DHCP client tries to renew its IP address after the expiration period, the client is redirected to the captive portal because its MAC address is no longer in the MAC address filter. For more information, see Defining MAC Address Filters.

If the user chooses to sign in as a guest, as shown in Figure 32.3, the user can fill in the guest registration page provided by the captive portal.

Figure 32.3 Stage 2b: Registering as a Guest
After the user signs in as a guest, the appliance stores the MAC address of the client in the MAC address filter for the guest range. When the DHCP client tries to renew its IP address, it receives a new IP address from the guest DHCP range, unless the MAC address of the client expired and was removed from the filter. In this case, the DHCP client is redirected to the captive portal.

### Configuring DHCP Authentication

Following are the tasks to configure the DHCP Authentication feature:

1. Configure the authentication server group which the captive portal uses to authenticate DHCP clients. For more information, see About Authentication Server Groups. If the captive portal is used to register guest users and does not authenticate users, then you do not have to configure an authentication server group.
2. Configure the captive portal properties and associate the captive portal with the authentication server group. For more information, see Configuring Captive Portal Properties.
3. Optionally, customize the captive portal interface and guest registration page, as described in Customizing the Captive Portal Interface. Additionally, if you enabled SSL encryption, upload the required certificates, as described in Managing Captive Portal Certificates.
4. Enable the captive portal, as described in Starting the Captive Portal Service.
5. Configure the network and a DHCP range for quarantine DHCP clients. Configure DHCP ranges for authenticated and guest DHCP clients, depending on whether you are allowing either one or both types of users to access your network. For information about configuring these DHCP ranges, see Defining the IPv4 Network and DHCP Ranges.
6. Run the Captive Portal wizard to create MAC address filters for the quarantine range and for the authenticated, and guest DHCP ranges, if configured; and to associate the captive portal server with the member that serves the DHCP ranges. To accomplish these tasks and set other properties, see Using the Captive Portal Wizard. Alternatively, you can perform these tasks separately or modify the configured properties, as described in Adding and Modifying the Filters and Associations.
7. Enable the DHCP service. For more information, see Starting DHCP Services on a Member.
About Authentication Server Groups

Create an authentication server group if you want the captive portal server to authenticate users when they register. You can create an authentication server group with RADIUS servers, LDAP servers, or Active Directory servers, and then associate the group with the member that runs the captive portal and sends the authentication requests. You can associate an authentication server group with multiple captive portals, but you can associate a captive portal with only one authentication server group.

The following sections provide instructions for creating a RADIUS authentication server group, an AD authentication server group and an LDAP server group:

- Configuring a RADIUS Authentication Server Group
- Configuring an Active Directory Authentication Server Group
- Configuring an LDAP Server Group

Configuring a RADIUS Authentication Server Group

You can add multiple RADIUS servers to an authentication server group and prioritize them. When the member sends an authentication request, it always selects the first RADIUS server in the list. It only sends authentication requests to the next server on the list if the first server goes down.

To configure the RADIUS authentication server group to which a captive portal server sends authentication requests:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Expand the Toolbar and click Add -> RADIUS Service.
3. In the Add RADIUS Authentication Service wizard, complete the following:
   - Name: Enter the name of the server group.
   - RADIUS Servers: Click the Add icon and enter the following:
     - Server Name or IP Address: Enter the RADIUS server FQDN or IP address.
     - Comment: You can enter additional information about the server.
     - Authentication Port: The destination port on the RADIUS server. The default is 1812.
     - Authentication Type: Select the authentication method of the RADIUS server from the drop-down list. You can specify either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol). The default is PAP.
     - Shared Secret: Enter the shared secret that the member DHCP server and the RADIUS server use to encrypt and decrypt their messages. This shared secret must match the one you entered on the RADIUS server.
     - Connect through Management Interface: Select this to enable the member to use its MGMT port to communicate with just this server.
     - Disable server: Select this to disable the RADIUS server if, for example, the connection to the server is down and you want to stop the DHCP server from trying to connect to this server.
     - Click Test to validate the configuration and check that the Grid Master can connect to the RADIUS server. Before you can test the configuration though, you must specify the authentication and accounting timeout and retry values. If the Grid Master connects to the RADIUS server using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the RADIUS server, the appliance displays a message indicating an error in the configuration.
   - Click Add to add the RADIUS server to the group.

When you add multiple RADIUS servers to the list, you can use the up and down arrows to change the position of the servers on the list. The member DHCP server connects to the RADIUS servers in the order they are listed.

- Authentication
- Timeout: The time that the member DHCP server waits for a response from a RADIUS server before considering it unreachable. You can enter the time in milliseconds or seconds. The maximum is 10 seconds.
- Retries: The number of times the member DHCP server retries connecting to a RADIUS server before it considers the server unreachable. The default is five.
- Accounting
- Timeout: The time that the member DHCP server waits for a response from a RADIUS server before considering it unreachable. You can enter the time in milliseconds or seconds. The maximum is 10 seconds.
- Recovery Interval: Specifies the duration of time a RADIUS server stays inactive after being down, before becoming eligible to have RADIUS requests sent to it. The recovery interval starts when a RADIUS server is first discovered to be down.
- Comment: You can enter additional information about the server group.
- Disable: Select this to disable the authentication server group.

4. Save the configuration and click Restart if it appears at the top of the screen.

Configuring an Active Directory Authentication Server Group

1. From the Administration tab, click the Authentication Server Groups tab.
2. Click the Active Directory Services subtab and click the Add icon.
3. In the Add Active Directory Authentication Service wizard, complete the following:
   - Name: Enter a name for the service.

For information about monitoring the captive portal and the DHCP service, see Monitoring DHCP Authentication.
• **Active Directory Domain**: Enter the AD domain name.

• **Domain Controllers**: Click the Add icon and complete the following to add an AD domain controller:
  - **Server Name or IP Address**: Enter the FQDN or the IP address of the AD server that is used for authentication.
  - **Comment**: Enter additional information about the AD server.
  - **Authentication Port**: Enter the port number on the domain controller to which the member sends authentication requests. The default is 389.
  - **Encryption**: Select SSL from the drop-down list to transmit through an SSL (Secure Sockets Layer) tunnel. When you select SSL, the appliance automatically updates the authentication port to 636. Infoblox strongly recommends that you select this option to ensure the security of all communications between the member and the AD server. If you select this option, you must upload a CA certificate from the AD server. Click **CA Certificates** to upload the certificate. In the **CA Certificates** dialog box, click the Add icon, and then navigate to the certificate to upload it.
  - **Connect through Management Interface**: Select this so that the member uses the MGMT port for administrator authentication communications with just this AD server.
  - **Disable server**: Select this to disable an AD server if, for example, the connection to the server is down and you want to stop the Grid member from trying to connect to this server.
  - **Click Test** to test the configuration. If the Grid member connects to the domain controller using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the server, the appliance displays a message indicating an error in the configuration.
  - **Click Add** to add the domain controller to the group.

• **Timeout(s)**: The number of seconds that the Grid member waits for a response from the specified authentication server. The default is 5.

• **Comment**: Enter additional information about the service.

• **Disable**: Select this to retain an inactive AD authentication service profile.

4. Save the configuration and click Restart if it appears at the top of the screen.

Managing Multiple Domain Controllers

You can create multiple domain controllers on the Microsoft server and associate it with a single Active Directory Domain, which is synchronized by multiple Grid members within the same Grid:

- Synchronization happens from only one Grid member that is a Microsoft server, which is referred as the master, at a time in a given network view.
- If the master Microsoft server fails the synchronization three times in a row, it loses its master status.
- The Grid Master will periodically ensure that for each Active Directory Domain there is one Microsoft server with the master status. Otherwise, the appliance selects a new master, based on the following:
  - Microsoft server that has been designated as the Grid Master for the longest time previously.
  - Microsoft server configured in read/write synchronization mode.
  - The master server is indicated within the Active Directory Domain object.
- Synchronization mode changes based on the master.
- When synchronization happens in two separate network views, respective Grid members synchronize data simultaneously.

About the Captive Portal

The captive portal can be used to register users for authentication, guest users, or both types of users. When a DHCP client attempts to connect to the network and its MAC address is not in any of the configured MAC filters, the member DHCP server assigns it an IP address in the quarantine range. When the quarantined client tries to reach any web site, it is redirected to the captive portal. The captive portal runs a limited DNS server that is used solely to redirect queries to the captive portal web interface. You can enable the captive portal as a service on any Grid member, except the Grid Master or Grid Master candidate. The Grid member that runs the captive portal cannot run any other service, such as DHCP and DNS. Note that the limited DNS service that the captive portal runs is different from the full-scale DNS service on an Infoblox appliance. The full-scale DNS service must be explicitly disabled on the member that runs the captive portal.

For information on disabling DNS service, see Configuring Captive Portal Properties. You can configure one or more captive portals in the Grid. You can also configure one or more member DHCP servers to use a captive portal to register users. For example, if your organization has two sites, you can configure a captive portal for each site and configure the DHCP servers in each site to use their respective captive portals to authenticate users.

In order for clients to reach the captive portal, you must specify a route to the captive portal. In a network where all IP addresses are on the same subnet, you can configure Option 33 for the quarantine DHCP range. For additional information, see Quarantine DHCP Range. On a routed network, you must configure a default route on the router for the subnet.

Following are the tasks to configure a captive portal:

1. Select the Grid member that runs the captive portal and configure its properties, as described in Configuring Captive Portal Properties.
2. Optionally, customize the captive portal and registrars.
3. If you enabled SSL, generate the CA certificate, as described in Managing Captive Portal Certificates.
4. Start the captive portal, as described in Starting the Captive Portal Service.

Configuring Captive Portal Properties

When you configure the captive portal properties of a member, you specify if it is used to register users for authentication, guests, or both. If it is used to register guests only, then do not associate it with an authentication server group.
You can specify the VIP address of the Grid member or configure an additional IP address on the loopback interface as the captive portal IP address. Alternatively, if the Grid member supports the LAN2 port and it is enabled, but the NIC failover feature is disabled, you can use the IP address of the LAN2 port as the captive portal IP address. To configure an IP address on the loopback interface, see Configuring IP Addresses on the Loopback Interface. For information on the LAN2 port, see Using the LAN2 Port.

In addition, you can configure the port on which the appliance listens for authentication requests redirected from the captive portal. When a user logs in to the captive portal, the member sends an authentication request to its associated authentication server group. The member determines future DHCP replies to client requests based on the authentication result.

To configure the properties of the captive portal:

1. From the Grid tab, select the Grid Manager tab, and then click Captive Portal.
2. Select the member that runs the captive portal and click the Edit icon.
3. In the General Basic tab of the Member Captive Portal Properties editor, complete the following:
   - **Use This Authentication Server Group for Authenticating Captive Portal Users:** Select the authentication server group that authenticates users for this captive portal. For information about authentication server groups, see About Authentication Server Groups.
   - **Captive Portal User Types:** Specify whether the captive portal is used to register Authenticated users only, Guest users only, or Both.
   - **Portal IP Address:** Select the IP address of the captive portal server. The appliance lists the VIP address and the IP addresses of the loopback interface and the LAN2 port, if enabled. You can select any of these addresses as the portal IP address.
   - **Enable SSL on Portal:** Select this to support encrypted web traffic through SSL/TLS. If you select this option, you must upload a certificate or generate a self-signed certificate. For information about creating and uploading a certificate for the captive portal, see Managing Captive Portal Certificates.
   - **Network View:** This field displays if there are multiple network views configured. Select the network view in which the authenticated, quarantine, and guest DHCP ranges belong.
   - **Log Registration Success:** Select to enable the member to log successful registrations in syslog, and then select the logging level from the drop-down list.
   - **Log Registration Failure:** Select to enable the member to log failed registrations in syslog, and then select the logging level from the drop-down list.

4. In the General Advanced tab of the editor, you can specify the port on which the member listens for authentication requests redirected from the captive portal. The default port is 4433. Depending on your firewall and network policies, you can configure an unused port greater than 1 and less than 63999.

5. Save the configuration and click Restart if it appears at the top of the screen.

Customizing the Captive Portal Interface

You can customize the captive portal, and if configured, the guest registration page as well. You can upload image files to the appliance and display your own logo, header and footer. In addition, you can upload the acceptable use policies that are displayed on the captive portal and guest registration page.

Following are guidelines for each item you can customize:

- **Logo Image:** The maximum size is 200 pixels wide by 55 pixels high, and the images can be in JPEG, GIF, or PNG format. It displays on top of the header image.
- **Header Image:** The optimal size is 600 pixels wide by 137 pixels high. The image can be in JPEG, GIF, or PNG format. The header displays at the top of the page.
- **Footer Image:** The optimal size is 600 pixels wide by 20 pixels high. The image can be in JPEG, GIF, or PNG format. The footer displays at the bottom of the page.
- **Acceptable Use Policy:** The policy must be saved as a UTF-8 encoded file. It appears below the welcome message in the captive portal. Users can scroll through the policy when they review it. This is used in the captive portal and guest registration page.

If any of the customizable fields are not configured, then the factory defaults are displayed. To customize the captive portal:

1. From the Grid tab, select the Grid Manager tab, and then click Captive Portal.
2. Select the member that is running the captive portal and click the Edit icon.
3. Select the Customization tab of the Member Captive Portal Properties editor.
4. In the General Captive Portal Customization section, complete the following:
   - **Company Name:** Enter the name of your company. The company name displays on the title bar of the browser. You can enter a maximum of 256 characters.
   - **Welcome Message:** Type the message that displays on the captive portal. The message can contain a maximum of 300 characters.
   - **Help Desk Message:** Type a message that provides Helpdesk information, such as contact information for technical assistance. The message can contain a maximum of 300 characters.
   - **Logo Image, Header Image, Footer Image, Acceptable Use Policy:** To display the image files and the acceptable use policy on the captive portal, click Select beside the item you want to upload. In the Upload dialog box, click Select File and navigate to the image or text file. Select the file you want to display and click Upload. Note that these files have size requirements, as listed earlier in this section.
5. In the **Guest Users Web Page Customization** section, complete the following:

- The appliance displays certain fields on the guest registration page. Select the check boxes of the fields that users are required to complete: **Require First Name**, **Require Middle Name**, **Require Last Name**, **Require Email**, and **Require Phone**.
- **Custom Field 1 — Custom Field 4**: You can display up to four additional fields on the guest registration page. To add a field to the guest registration page, enter a label for that field. The label can have a maximum of 32 characters. Select **Require** to require users to complete the field.

Users can enter a maximum of 128 characters in each of the fields in the captive portal login page and the guest registration page.

6. Save the configuration and click **Restart** if it appears at the top of the screen.

**Managing Captive Portal Certificates**

When you enable support for encrypted web traffic sent over SSL/TLS, you can do any of the following:

- Generate a self-signed certificate and save it to the certificate store of your browser.
- Request a CA-signed certificate. When you receive the certificate from the CA, upload it on the member running the captive portal.

**Generating Self-Signed Certificates**

You can generate a self-signed certificate for the captive portal. When you generate a self-signed certificate, you can specify the hostname and change the public/private key size, enter valid dates and specify additional information specific to the captive portal. If you have multiple captive portals, you can generate a certificate for each captive portal with the appropriate hostname.

To generate a self-signed certificate:

1. From the Grid tab, select the Grid Manager tab, and then click Captive Portal.
2. Select the member that is running the captive portal, and then click HTTPS Cert -> Generate Self-signed Certificate from the Toolbar.
3. In the Generate Self-signed Certificate dialog box, complete the following:
   - **Secure Hash Algorithm and Key Size**: You can select SHA-1 and a RSA key size of 1024 or 2048. SHA-256 (SHA-2) can be selected together with a RSA key size of 2048 or 4096. The default value is SHA-256 2048.
   - **Days Valid**: Specify the validity period of the certificate.
   - **Common Name**: Specify the domain name of the captive portal.
   - **Organization**: Enter the name of your company.
   - **Organizational Unit**: Enter the name of your department.
   - **Locality**: Enter a location, such as the city or town of your company.
   - **State or Province**: Enter the state or province.
   - **Country Code**: Enter the two-letter code that identifies the country, such as US.
   - **Admin E-mail Address**: Enter the email address of the captive portal administrator.
   - **Comment**: Enter additional information about the certificate.

4. Click **OK**.

**Generating Certificate Signing Requests**

You can generate a CSR (certificate signing request) that you can use to obtain a signed certificate from your own trusted CA. Once you receive the signed certificate, you can import it in to the Grid member that runs the captive portal, as described in **Uploading Certificates**.

To generate a CSR:

1. From the Grid tab, select the Grid Manager tab, and then click Captive Portal.
2. Select the member that is running the Captive Portal, and then click HTTPS Cert -> Create Signing Request from the Toolbar.
3. In the Create Signing Request dialog box, enter the following:
   - **Secure Hash Algorithm and Key Size**: You can select SHA-1 and a RSA key size of 1024 or 2048. SHA-256 (SHA-2) can be selected together with a RSA key size of 2048 or 4096. The default value is SHA-256 2048.
   - **Common Name**: Specify the domain name of the captive portal.
   - **Organization**: Enter the name of your company.
   - **Organizational Unit**: Enter the name of your department.
   - **Locality**: Enter a location, such as the city or town of your company.
   - **State or Province**: Enter the state or province.
   - **Country Code**: Enter the two-letter code that identifies the country, such as US.
   - **Admin E-mail Address**: Enter the email address of the captive portal administrator.
   - **Comment**: Enter additional information about the certificate.

4. Click **OK**.

**Uploading Certificates**

When you upload a certificate, the NIOS appliance finds the matching CSR and takes the private key associated with the CSR and associates it
with the newly uploaded certificate. The appliance then automatically deletes the CSR.
If the CA sends an intermediate certificate that must be installed along with the server certificate, you can upload both certificates to the appliance. The appliance supports the use of intermediate certificates to complete the chain of trust from the server certificate to a trusted root CA.
To upload a certificate:

1. From the Grid tab, select the Grid Manager tab, and then click Captive Portal.
2. Select the member that is running the captive portal, and then click HTTPS Cert -> Upload Certificate from the Toolbar.
3. In the Upload dialog box, click Select File, navigate to the certificate location, and click Open.

The appliance imports the certificate. When you log in to the appliance again, it uses the certificate you imported.

Downloading Certificates
You can download the current certificate or a self-signed certificate so users can install it in their browsers. To download a certificate:

1. From the Grid tab, select the Grid Manager tab, and then click Captive Portal.
2. Select the member that is running the captive portal, and then click HTTPS Cert -> Download Certificate from the Toolbar.
3. Navigate to where you want to save the certificate and save it.

Starting the Captive Portal Service
Before you start the captive portal service, ensure that the member is not running any other service. To start the captive portal service:

1. From the Grid tab, select the Grid Manager tab, and then click Captive Portal.
2. Select the member that is configured to run the captive portal service and click the Start icon.

Defining the IPv4 Network and DHCP Ranges
First define the IPv4 network that uses DHCP authentication, and then define the DHCP ranges and services for each access level that you want to provide on the network:

- Quarantine
- Authenticated
- Guest

For information about configuring DHCP IPv4 networks, ranges and services, see Chapter 27, Managing IPv4 DHCP Data, and Chapter 26, Configuring DHCP Properties.

Quarantine DHCP Range
You must configure a DHCP range for the quarantine level so the member DHCP server can assign IP addresses within that range to unauthenticated DHCP clients. An unauthenticated client is allowed to access the captive portal only and must successfully pass the authentication process before it can receive an IP address from the authenticated range.
Infoblox recommends 30-second leases for addresses in the quarantine DHCP range. This provides enough time for the user authentication process, so when the client attempts to renew the lease at the midpoint of its lease time, the member can then assign the client a new IP address, depending on the result of the authentication process.
When you configure the quarantine DHCP range, you must specify the captive portal IP address as the DNS server for the address range. The captive portal runs a limited DNS server that resolves all queries with the IP address assigned to the web interface on the captive portal.
Note that you can run the Captive Portal wizard to automatically set the lease time of the quarantine range to 30 seconds and to add the captive portal IP address as the DNS server. For information about the Captive Portal wizard, see Using the Captive Portal Wizard. Alternatively, you can set the lease time and the DNS server IP address in the DHCP tab of the DHCP Range editor. For information about the DHCP Range editor, see Configuring IPv4 Address Ranges.
To ensure that clients can reach the captive portal, you must specify a route to the captive portal. On a network where all systems can reach each other without going through a router, that is, all IP addresses are on the same subnet, you must configure Option 33 for the quarantine DHCP range. This option specifies a list of static routes that the client should install in its routing cache. The routes consist of a list of IP address pairs. For clients to reach the captive portal, specify the portal IP address first (destination address), and the LAN address of the NIOS appliance second. When the appliance assigns an IP address from the quarantine DHCP range, it also includes the static route that you specified in option 33. For information about configuring DHCP options, see Configuring IPv4 DHCP Options. On a routed network, you must configure a default route via the router on the subnet.

Authenticated DHCP Range
Configure a DHCP range for authenticated users if you want the Grid member to assign IP addresses within that range to authenticated DHCP clients. Users that receive an IP address in this range typically are allowed full access to the network.
When a client successfully passes authentication, the member automatically stores its MAC address in the corresponding MAC address filter.
When the client attempts to renew the lease at the midpoint of its lease time, the member matches the source MAC address in the request with a MAC address in the filter for the authenticated DHCP address range. The member then assigns the client a new IP address from the authenticated DHCP range.

Guest DHCP Range

Configure a guest DHCP range if you want to provide guest access privileges. You can configure and customize a guest registration page when you configure the captive portal. For information about this feature, see Customizing the Captive Portal Interface.

Defining MAC Address Filters

After you configure the network and DHCP ranges, you must then configure the MAC address filters and add them to the appropriate DHCP ranges. If you configured DHCP ranges for authenticated and guest users, you must configure MAC address filters for each range with an action of Allow. You must also add those filters to the quarantine range with an action of Deny, to ensure that the member does not allocate an address from the quarantine range to a host whose MAC address matches an entry in the MAC filters for the authenticated and guest DHCP ranges. When you create the filters, you also specify whether the MAC address entries expire. The member automatically deletes expired MAC address entries from the filter. If a client that registered earlier attempts to renew its IP address or to register after its MAC address has expired, it is redirected to the captive portal because its MAC address is no longer in the filter.

You can run the Captive Portal wizard to automatically create the MAC address filters, as described in the next section, Using the Captive Portal Wizard, or you can configure each filter as described in Defining MAC Address Filters.

Using the Captive Portal Wizard

After you configure the captive portal and the DHCP ranges for each access level, you can use the Captive Portal wizard to accomplish the following tasks:

- Associate the captive portal member with the member that serves the DHCP ranges you configured.
- Create MAC address filters and add them to the appropriate DHCP ranges. The wizard allows you to create MAC address filters for the quarantine DHCP range, and for the authenticated and guest DHCP ranges, depending on whether the captive portal is used to register users for authentication, guests, or both. This was specified, when you configured the captive portal properties, described in Configuring Captive Portal Properties. For example, if you indicated that the captive portal is used for authenticated users only, then the wizard allows you to create a MAC filter for the authenticated DHCP range only.
- If the captive portal is used to register users for authentication, the wizard allows you to create a MAC address filter for the authenticated range. The wizard then automatically adds the filter to the authenticated DHCP range with an action of Allow. It also adds the filter to the quarantine range with an action of Deny. This ensures that the member does not allocate an address from the quarantine range to a host whose MAC address matches an entry in the MAC filter.
- If the captive portal is used to register guest users, the wizard allows you to create a MAC address filter for the guest range. The wizard then automatically adds the filter to the guest DHCP range with an action of Allow. It also adds the filter to the quarantine range with an action of Deny. This ensures that the member does not allocate an address from the quarantine range to a host whose MAC address matches an entry in the MAC filter.
- Add the captive portal IP address as the DNS server for the quarantine address range.
- Set the lease time of the quarantine range to 30 seconds.

To use the Captive Portal wizard to complete the tasks for the DHCP authentication feature:

1. From the Data Management tab, select the DHCP tab, or from the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and click Configure Captive Portal.
3. In the Captive Portal wizard, complete the following and click Next:
   - **Member DHCP**: Select the member DHCP server that uses this captive portal to authenticate users.
   - **Captive Portal**: Select the member that runs the captive portal. Note that the member that runs the captive portal cannot run any other service, such as DHCP or DNS, and cannot be the Grid Master or Grid Master candidate.
4. This panel allows you to create MAC filters for the authenticated and guest DHCP ranges. The MAC filters you can create depend on your entry in the Captive Portal properties of the Grid member. For example, if you indicated that the captive portal is used for authenticated users only, then this panel allows you to create a MAC filter for the authenticated DHCP range only.

   You can also specify existing MAC filters, if you want to apply them to the authenticated and guest DHCP ranges. Complete the following and click Next:

   - **Authenticated MAC Filter**: Specify a name for the MAC filter that is used for authenticated users.
   - **Expiration Time**: Specify how long a MAC address is stored in the MAC address filter for authenticated users.
     - **Never**: Select this option to store MAC addresses in the MAC address filter until they are manually removed.
     - **Expires in**: Select this option to store MAC addresses in the MAC address filter for the specified period of time.
   - **Guest MAC Filter**: Specify a name for the MAC filter that is used for guest users.
   - **Expiration Time**: Specify how long a MAC address is stored in the MAC address filter for guest users.
     - **Never**: Select this option to store MAC addresses in the MAC address filter until they are manually removed.
     - **Expires in**: Select this option to store MAC addresses in the MAC address filter for the specified period of time.

5. In this panel, you specify the network and address ranges, so the wizard can apply the MAC address filters to the appropriate ranges. Complete the following:

   - **Network**: Select the network that uses DHCP authentication.
**Authenticated Range:** Select the IP address range that the appliance uses for authenticated users. The wizard applies the authenticated MAC address filter you specified in the preceding step to this DHCP range with an action of Allow. This effectively allows the member to assign an IP address from the address range to a requesting host whose MAC address matches the MAC address in the filter.

**Guest Range:** Select the IP address range that the appliance uses for guest users. The wizard applies the guest MAC address filter you specified in the preceding step to this DHCP range with an action of Allow. This effectively allows the member to assign an IP address from the address range to a requesting host whose MAC address matches the MAC address in the filter.

**Quarantine Range:** Select the IP address range that the appliance uses for quarantined addresses. The wizard applies the authenticated and guest MAC address filters to the quarantine DHCP range with an action of Deny. This effectively denies an address request from a host whose MAC address matches an entry in the MAC filters for the authenticated and guest DHCP ranges.

6. Save the configuration and click Restart if it appears at the top of the screen.

**About Authentication Servers**

You can create a RADIUS authentication server group for Sophos NAC Advanced servers, and then associate the group with the member DHCP server that sends authentication requests. The member DHCP server tries to connect to each Sophos NAC Advanced server in the group using one of the following methods: Ordered List or Round Robin.

In the Ordered List method, the member DHCP server always selects the first Sophos NAC Advanced server in the list when it sends an authentication request. It only sends authentication requests to the next server on the list if the first server goes down. In the Round Robin method, the member DHCP server selects the first Sophos NAC Advanced server for the first request, the second server for the next request, and so on until it selects the last server in the list. Then it starts with the first server in the list and continues the same selection process.

Each member DHCP server can have only one RADIUS server group assigned, but a RADIUS server group can be assigned to multiple member DHCP servers.

**Adding a Server Group**

To create a RADIUS authentication server group for Sophos NAC Advanced servers:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Expand the Toolbar and click Add -> RADIUS Service.
3. In the Add RADIUS Authentication Service wizard, complete the following:
   - **Name:** Enter the name of the server group.
   - **RADIUS Servers:** Click the Add icon and enter the following:
     - **Server Name or IP Address:** Enter the Sophos NAC Advanced server FQDN or IP address.
     - **Comment:** You can enter additional information about the server.
     - **Authentication Port:** The destination port on the Sophos NAC Advanced server. The default is 1812.
     - **Authentication Type:** Select the authentication method of the RADIUS server from the drop-down list. You can specify either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol). The default is PAP.
     - **Shared Secret:** Enter the shared secret that the member DHCP server and the Sophos NAC Advanced server use to encrypt and decrypt their messages. This shared secret must match the one you entered on the Sophos NAC Advanced server.
     - **Enable Accounting:** Leave this blank. RADIUS accounting is not supported.
     - **Connect through Management Interface:** Select this so that the NIOS appliance uses the MGMT port for communications with just this server.
     - **Disable server:** Select this to disable the Sophos NAC Advanced server if, for example, the connection to the server is down and you want to stop the DHCP server from trying to connect to this server.
     - **Click Test** to validate the configuration and check that the Grid Master can connect to the Sophos NAC Advanced server. Before you can test the configuration though, you must specify the authentication and accounting timeout values. If the Grid Master connects to the Sophos NAC Advanced server using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the Sophos NAC Advanced server, the appliance displays a message indicating an error in the configuration.
     - **Click Add to add the Sophos NAC Advanced server to the server group.**

When you add multiple Sophos NAC Advanced servers to the list, you can use the up and down arrows to change the position of the servers on the list. The member DHCP server connects to the Sophos NAC Advanced servers in the order they are listed.

- **Authentication**
- **Timeout:** The time that the member DHCP server waits for a response from a Sophos NAC Advanced server before considering it unreachable. You can enter the time in milliseconds or seconds.
- **Retries:** The number of times the member DHCP server retries connecting to a Sophos NAC Advanced server before it considers the server unreachable. The default is five.
- **Mode:** Specifies how the member DHCP server selects the first Sophos NAC Advanced server to contact.
  - **Ordered List:** The member DHCP server always selects the first Sophos NAC Advanced server in the list when it sends an authentication request. It queries the next server only when the first server is considered down. This is the default.
  - **Round Robin:** The member DHCP server selects the first Sophos NAC Advanced server for the first request, the second server for the next request, and so on. If the last server is reached, then the DHCP server starts with the first server.
server in the list, and so on.

- **Enable Authentication Cache**: The member DHCP server automatically caches authentication results for 120 seconds. When you enable this option, you can override this default in the Cache Time to Live field. You must enable this option to clear the cache, as described in Clearing the Authentication Cache.
- **Cache Time to Live**: Specifies the duration of time an authentication result is stored. The default is one hour. The maximum is 259200 seconds (3 days).
- **Recovery Interval**: Specifies the duration of time a Sophos NAC Advanced server stays inactive after being down, before becoming eligible to have RADIUS requests sent to it. The recovery interval starts when a Sophos RADIUS server is first discovered to be down.
- **Comment**: You can enter additional information about the server group.
- **Disable**: Select this to disable the authentication server group.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Associating a Server Group with a Member

To associate an authentication server group with a member DHCP server:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box, and click the **Edit** icon.
2. If the **Member DHCP Properties** editor is in Basic mode, click **Toggle Expert Mode**.
3. Select the **IPv4 Authenticated DHCP** tab.
4. Click the **Use this Authentication Server Group for Sophos/RAIDIUS Authenticated DHCP** check box, and then select a group from the drop-down list.
5. Save the configuration and click **Restart** if it appears at the top of the screen.

### Managing Server Groups

To view the list of authentication server groups, from the **Administration** tab, click the **Authentication Server Groups** tab and expand the **RadiantUS Service** subtab. For each server group, you can view the server group name, comments, and whether the group is available or disabled. You can then select a server group to modify or delete it.

To modify a server group, select it and click the **Edit** icon. You can modify any of its properties, and add or delete servers from the group. When you delete a Sophos NAC Advanced server from a group, the appliance permanently deletes it.

To delete a server group, select it and click the **Delete** icon. When you delete an authentication server group, the appliance permanently deletes it.

### Clearing the Authentication Cache

The authentication cache can store authentication results for up to 20,000 DHCP clients. When the cache reaches its limit, the DHCP member logs a message in syslog. To clear the entire cache or the cache entry of a specific MAC address, you must enable the authentication cache in the RADIUS Service wizard or editor.

To clear the entire authentication cache:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box.
2. Expand the Toolbar and select **Clear Authentication Cache**.
3. When the **Clear Authentication Cache** confirmation dialog appears, click **Purge**.

To delete a specific entry:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box.
2. Expand the Toolbar and select **Clear Authentication Record**.
3. In the **Clear Authentication Record** dialog box, enter the DHCP client MAC address, and then click **Purge**.

### Adding and Modifying the Filters and Associations

The Captive Portal wizard simplified the configuration process by accomplishing a number of tasks simultaneously. To accomplish each task separately, or to modify the filters or associations after you have run the wizard:

- To define the MAC address filters for each range, see **Defining MAC Address Filters**.
- To bind each filter to the appropriate DHCP range, see **Applying Filters to DHCP Objects**.
- To specify the DNS server IP address for the quarantine range and set the lease time to 30 seconds, see **Configuring General IPv4 DHCP Properties**.
- To associate a member DHCP server with a captive portal and specify the MAC filters for the authenticated and guest DHCP ranges:
  a. From the **Data Management** tab, select the **DHCP** tab -> **Members** tab -> **member** check box -> **Edit** icon.
  b. In the **Member DHCP Properties** editor, click the **IPv4 Authenticated DHCP** tab and complete the following:
    - **Use this Captive Portal for Infoblox Authenticated DHCP**: Select this check box and select the captive portal that
you want to associate with the member.

- **Authenticated User MAC Filter**: Select the MAC filter used for authenticated users. To change your section, click **Clear** and click **Select** again.
- **Guest User MAC Filter**: Select the MAC filter for guest users. To change your selection, click **Clear** and click **Select** again.

c. Save the configuration and click **Restart** if it appears at the top of the screen.

**Monitoring DHCP Authentication**

You can monitor the status of the captive portal service, as described in Monitoring Services. You can check its status in the Grid Status widget and the Member Status widget on the Dashboard. For information about these widgets, see Chapter 2, Dashboards.

You can also view the MAC addresses that were added to each MAC address filter, as described in Viewing MAC Address Filter Items.

**Viewing DHCP Ranges and Filters**

To view the newly created MAC address filters:

1. From the **Data Management** tab, select the **DHCP** tab -> **IPv4 Filters** tab. Grid Manager lists all the configured filters.
2. You can select a filter and view or configure its properties, such as extensible attributes.

For more information about the filters and editing their properties, see Managing DHCP Filters.

To view the DHCP ranges and the newly added filters:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** section -> **network**.
2. Select the DHCP range you want to view and click the Edit icon.
3. If the editor is in Basic mode, click **Toggle Expert Mode**.
4. Click the **Filters** tab to view the filters.

To verify that the captive portal is the DNS server in the quarantine range:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** section -> **network**.
2. Select the quarantine DHCP range and click the Edit icon.
3. In the **DHCP Range** editor, click the **DHCP** tab.

The captive portal IP address is listed in the DNS Servers table.

**Configuration Example: Configuring Authenticated DHCP**

In this example, a school (school.edu) has two locations, its main campus, campus1.school.edu, and a satellite campus, campus2.school.edu. It has a captive portal server in each location. In the main campus, the Grid Master also functions as a DHCP server and uses a captive portal server to register DHCP clients. In the satellite campus, two members serve DHCP and use the same captive portal server. The captive portal servers use the same RADIUS authentication server group to authenticate users.
Create the RADIUS Authentication Server Group

Create the RADIUS authentication server group and add two RADIUS servers to the group.

1. From the Administration tab, click the Authentication Server Groups tab.
2. Expand the Toolbar and click Add -> RADIUS Service.
3. In the Add RADIUS Authentication Service wizard, complete the following:

   - **Name**: Enter RADIUS ASG.
   - **RADIUS Servers**: Click the Add icon and enter the following:
     - **Server Name or IP Address**: Enter the RADIUS server FQDN, which is rs1.school.edu.
     - **Authentication Port**: Accept the default port (1812).
     - **Authentication Type**: Select the PAP authentication method.
     - **Shared Secret**: Enter no1nose.
   - **Authentication**:
     - **Timeout**: Enter 5 seconds.
     - **Retries**: Accept the default, which is five.
   - **Accounting**:
     - **Timeout**: Enter 5 seconds.
     - **Retries**: Accept the default, which is five.
     - **Click Test to validate the configuration and check that the Grid Master can connect to the RADIUS server.
Grid Manager displays a message confirming the configuration is valid. 

**Add** to add another RADIUS server to the group, and then enter the following:

- **Server Name or IP Address**: Enter the RADIUS server FQDN, which is `rs2.school.edu`.
- **Authentication Port**: Accept the default port (1812).
- **Authentication Type**: Select the PAP authentication method.
- **Shared Secret**: Enter `no1nose`.

- **Authentication**
  - **Timeout**: Enter 5 seconds.
  - **Retries**: Accept the default, which is five.

- **Accounting**
  - **Timeout**: Enter 5 seconds.
  - **Retries**: Accept the default, which is five.
  - Click **Test** to validate the configuration and check that the Grid Master can connect to the RADIUS server.

4. Click **Save & Close**.

### Configure the Captive Portal Properties

Configure the captive portal properties of `cp1.campus1.school.edu`.

1. From the **Grid** tab, select the **Grid Manager** tab.
2. Click the **Captive Portal** tab -> **Services** tab.
3. Select the member `cp1.campus1.school.edu` and click the **Edit** icon.
4. In the **General** tab of the **Member Captive Portal Properties** editor, complete the following:
   - **Use This Authentication Server Group for Authenticating Captive Portal Users**: Select `RADIUS ASG`.
   - **Captive Portal User Types**: Select `Both`.
   - **Portal IP Address**: Select `10.2.2.10`.
   - **Enable SSL on Portal**: Select this option.
   - **Log Registration Success**: Select `Informational`.
   - **Log Registration Failure**: Select `Informational`.
5. Click **Save & Close**.

Configure the captive portal properties of `cp2.campus2.school.edu`.

1. From the **Grid** tab, select the **Grid Manager** tab.
2. Click the **Captive Portal** tab -> **Services** tab.
3. Select the member `cp2.campus2.school.edu` and click the **Edit** icon.
4. In the **General** tab of the **Member Captive Portal Properties** editor, complete the following:
   - **Use This Authentication Server Group for Authenticating Captive Portal Users**: Select `RADIUS ASG`.
   - **Captive Portal User Types**: Select `Both`.
   - **Portal IP Address**: Select `10.1.3.10`.
   - **Enable SSL on Portal**: Select this option.
   - **Log Registration Success**: Select `Informational`.
   - **Log Registration Failure**: Select `Informational`.
5. Click **Save & Close**.

### Customize the Captive Portals

Customize the captive portal `cp1.campus1.school.edu`.

1. From the **Grid** tab, select the **Grid Manager** tab.
2. Click the **Captive Portal** tab-> **Services** tab.
3. Select `cp1.campus1.school.edu` and click the **Edit** icon.
4. Select the **Customization** tab of the **Member Captive Portal Properties** editor.
5. In the **General Captive Portal Customization** section, complete the following:
   - **Company Name**: Enter `School`.
   - **Welcome Message**: Type the following: `Welcome to School. Please sign in.`
   - **Help Desk Message**: Type: `To reach the Helpdesk, call (408) 111-2222 or email helpdesk@school.edu`.
   - **Logo Image**: Click **Select** beside the logo file and upload it.
6. In the **Guest Users Web Page Customization** section, complete the following:
   - Select the check boxes beside **Require First Name**, **Require Last Name**, **Require Email**.
7. Click **Save & Close**.

Select the other captive portal server, `cp2.campus2.school.edu`, and enter the same information.

### Generate a Self-Signed Certificate and Upload It
To generate a self-signed certificate for cp1.campus1.school.edu:

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab from the Services tab.
3. Select cp1.campus1.school.edu, and then click HTTPS Cert -> Generate Self-signed Certificate from the Toolbar.
4. In the Generate Self-signed Certificate dialog box, complete the following:
   - Secure Hash Algorithm and Key Size: You can select SHA-1 and a RSA key size of 1024 or 2048. SHA-256 (SHA-2) can be selected together with a RSA key size of 2048 or 4096. The default value is SHA-256 2048.
   - Days Valid: Enter 60 days.
   - Common Name: Enter cp1.campus1.school.edu.
5. Click OK.
6. Click Save & Close.

To generate a self-signed certificate for the captive portal cp2.campus2.school.edu:

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab from the Services tab.
3. Select cp2.campus2.school.edu, and then click HTTPS Cert -> Generate Self-signed Certificate from the Toolbar.
4. In the Generate Self-signed Certificate dialog box, complete the following:
   - Secure Hash Algorithm and Key Size: You can select SHA-1 and a RSA key size of 1024 or 2048. SHA-256 (SHA-2) can be selected together with a RSA key size of 2048 or 4096. The default value is SHA-256 2048.
   - Days Valid: Enter 60 days.
   - Common Name: Enter cp2.campus2.school.edu.
5. Click OK.
6. Click Save & Close.

Start the Captive Portal Service

1. From the Grid tab, select the Grid Manager tab.
2. Click the Captive Portal tab from the Services tab.
3. Select cp1.campus1.school.edu and cp2.campus2.school.edu, and then click the Start icon.

Configure the Networks and DHCP Ranges

Configure the network on the Grid Master.

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section.
2. Click the Add drop-down list and select IPv4 Network.
3. In the Add IPv4 Network wizard, select one of the following and click Next:
   - Add Network: Click this.
4. Complete the following and click Next:
   - Address: Enter 10.2.1.0/24.
5. Complete the following to assign the network to the Grid Master:
   - Add Infoblox Member: Select gm.campus1.school.edu.
6. Click Save & Close.

Configure the ranges on the Grid Master. To create the authenticated range:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks section.
2. Click the 10.2.1.0/24 network link, and then click the Add drop-down list and select DHCP Range.
3. In the Add IPv4 Range wizard, select Add DHCP Range and click Next.
4. Complete the following:
   - Network: Click Select Network and select 10.2.1.0/24.
   - Start: Enter 10.2.1.50. End: Enter 10.2.1.150.
   - Name: Enter authenticated range.
5. Click Next and complete the following:
   - Grid Member: Select this option and select gm.campus1.school.edu.
6. Click Save & Close.

To create the guest range:

1. Click the 10.2.1.0/24 network link, and then click the Add drop-down list and select DHCP Range.
2. In the Add IPv4 Range wizard, select Add DHCP Range and click Next.
3. Complete the following:
Network: Click Select Network and select 10.2.1.0/24.
Start: Enter 10.2.1.151.
End: Enter 10.2.1.170.
Name: Enter guest range.

4. Click **Next** and complete the following:
   
   * Grid Member: Select this option and select gm.campus1.school.edu.

5. Click **Save & Close**.

To create the quarantine range:

1. Click the 10.2.1.0/24 network link, and then click the Add drop-down list and select DHCP Range.
2. In the Add IPv4 Range wizard, select **Add DHCP Range** and click **Next**.
3. Complete the following:
   
   * Network: Click Select Network and select 10.2.1.0/24.
   * Start: Enter 10.2.1.225.
   * End: Enter 10.2.1.254.
   * Name: Enter quarantine range.

4. Click **Next** and complete the following:
   
   * Grid Member: Select this option and select gm.campus1.school.edu.

5. Click **Save & Close**.

Create the network and DHCP ranges for the DHCP servers ds1.campus1.school.edu and ds2.campus2.school.edu.

Run the Captive Portal Wizard

Run the Captive Portal wizard to associate the Grid Master with its captive portal, and to configure the MAC address filters:

1. From the Data Management tab, select the DHCP tab, or from the Grid tab, select the Grid Manager tab.
2. Expand the Toolbar and click Configure Captive Portal.
3. In the Captive Portal wizard, complete the following and click **Next**:
   
   * Member DHCP: Select the Grid Master, gm.campus1.school.edu.
   * Captive Portal: Select cp1.campus1.school.edu.
4. Complete the following and click **Next**:
   
   * Authenticated MAC Filter: Enter Auth_MAC_Filter.
   * Expiration Time: Select Never.
   * Guest MAC Filter: Enter Guest_MAC_Filter.
   * Expiration Time: Select Never.
5. Complete the following:
   
   * Network: Select 10.2.1.0/24.
   * Authenticated Range: Select 10.2.1.50 - 10.2.1.150.
   * Guest Range: Select 10.2.1.151 - 10.2.1.170.
   * Quarantine Range: Select 10.2.1.225 - 10.2.1.254.

6. Click **Save & Close**.

Run the Captive Portal wizard to associate ds1.campus2.school.edu with the captive portal server cp2.campus2.school.edu, and then run it again to associate ds2.campus2.school.edu with the same captive portal server.

Start the DHCP Service

To start the DHCP service on the Grid Master:

1. From the Data Management tab, select the DHCP tab -> Members tab.
2. Select the Grid Master gm.campus1.school.edu, and the two members, ds1.campus2.school.edu and ds2.campus2.school.edu.
3. Expand the Toolbar and click **Start**.
4. In the Start Member DHCP Service dialog box, click **Yes**.
5. Grid Manager starts DHCP services on the Grid Master and on the selected members.

NAC Integration

You can configure member DHCP servers to send authentication requests to RADIUS servers and to allocate addresses based on the authentication results. This allows you to place DHCP clients into separate network segments.

You can divide your network into different segments by configuring address ranges and applying NAC filters to them. NAC filters use authentication results from RADIUS servers as matching criteria for granting or denying address requests.
When a DHCP client requests a lease, the member DHCP server can query a remote backend RADIUS server such as the Sophos NAC Advanced server to determine if the DHCP client is authorized to access the network. A Sophos NAC Advanced server is an access-control and compliance server that supports the RADIUS protocol. The RADIUS server then checks its database and provides the compliance state and user class, if configured, of the DHCP client. The member DHCP server matches the response with the configured NAC filters, and grants a lease to the appropriate network segment.

Figure 32.5 presents an example illustrating the authentication process and how a member DHCP server matches the response with NAC filters to determine whether to grant or deny a lease. In the example, there are two DHCP ranges configured, each with a NAC filter that specifies RADIUS compliance state of DHCP clients allowed in each range.

### Configuring NAC with RADIUS Servers

Complete the following tasks to configure the RADIUS server and the member DHCP server. On an already functioning RADIUS server:

1. Add the member DHCP server as a RADIUS client. Make sure that the shared secret you enter on the RADIUS server matches the shared secret that you specify when you add the server to the authentication server group in Grid Manager. Note that on Grid Manager, you can enter only one shared secret for each RADIUS server. Therefore, on a RADIUS server, you must define the same shared secret for all Grid members that connect to it. For information about adding RADIUS clients, refer to the documentation for the RADIUS server.
2. Add the Infoblox Grid Master as a RADIUS client, even if it is not going to perform NAC authentication. This enables you to test the connection to the RADIUS server.

On the member DHCP server:

1. Configure the network and the DHCP ranges. For information, see Configuring DHCP Ranges.
2. Configure the NAC filters, as described in Applying Filters to DHCP Objects.
3. Enable the DHCP service. For information, see Starting DHCP Services on a Member.
Optionally, you can do the following:

- Manage the authentication cache, as described in Clearing the Authentication Cache.

### Configuring DHCP Ranges

Create the IPv4 network and DHCP ranges as described in Chapter 27, Managing IPv4 DHCP Data. You can create multiple DHCP ranges and apply one or more NAC filters to each of them.

### Listing DHCP Ranges

By default, DHCP ranges are listed according to their start addresses. You can reorder them according to the order in which you want the member DHCP server to evaluate the ranges.

Consider the following sample DHCP ranges:

- 10.20.30.100-10.20.30.199 (NAC filter that allows leases for compliant DHCP clients)
- 10.20.30.0-10.20.30.99 (No filters)

If the DHCP range with the NAC filter is listed before the range with no filters, then the DHCP server consults the Sophos NAC Advanced server and applies the NAC filter before it grants a lease. It grants leases from the range with no filters only if no NAC filters matched or after all leases from the first range are exhausted. If the first range is the production range and the second range is for the quarantine group, then the server applies the NAC filters for the production range, before it grants leases to the quarantine range.

To change the order of DHCP ranges in a network:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> network.
2. Expand the Toolbar and click Order DHCP Ranges.
3. In the Order DHCP Ranges dialog box, click the up and down arrows to move ranges up or down on the list. The Priority value changes accordingly.
4. Click OK.

You can view the DHCP objects in a network, including its DHCP ranges by navigating to the DHCP tab -> Networks tab -> Networks panel, and then clicking the network link. You can select the Priority column for display to view the order of the DHCP ranges. For information about editing the columns, see Customizing Tables.

### About NAC Filters

You can define NAC filters that specify authentication results from a remote, backend RADIUS server such as the Sophos NAC Advanced server. You can then apply each filter to a DHCP range or range template and indicate whether the DHCP server grants or denies a lease when the authentication result matches the filter. You can apply NAC filters to any DHCP range and DHCP range template.

NAC filters are enabled by default. When necessary, you can disable them for the entire Grid so you can perform maintenance on your RADIUS server. When you disable NAC filters, no service interruptions, service down times, configuration changes, or server restarts are required. For information about how to disable NAC filters, see 5800276 5800276.

In a NAC filter, you can define rules that specify the following:

- The status of the RADIUS authentication server group:
  - Success: At least one of the servers in the RADIUS authentication server group is up.
  - Fail: The MAC address in the DHCP request is not in the authentication cache and all servers in the server group are down.
  - Disabled: The RADIUS authentication server group is disabled, all the servers in the group are disabled, or the member is not assigned a server group.

- The response from the RADIUS server:
  - Accept: The response is an Access-Accept packet.
  - Reject: The response is an Access-Reject packet.

- Whether the Access-Accept packet contains an error. The Infoblox DHCP server expects certain RADIUS VSAs in the Access-Accept packet. An error occurs when any of the RADIUS VSAs are missing. For information about the Access-Accept packet and the RADIUS VSAs, refer to the documentation for the specified RADIUS server.
  - Yes: The Access-Accept packet does not include one or more RADIUS VSAs.
  - No: There are no errors in the Access-Accept packet.

- A compliance state: unknown, non-compliant, compliant or partially compliant

- A RADIUS server user class

When the member DHCP server receives an address request, it checks the DHCP ranges in their priority order. For information about the order of DHCP ranges, see Listing DHCP Ranges.

For each DHCP range, it checks if the request matches any MAC filters, relay agent filters, or DHCP option filters that apply to the range. (For information about these filters, see Chapter 31, Configuring IPv4 DHCP Filters.) If any of those filters match, then the member either grants or denies a lease to the DHCP client, based on the filter. If none of those filters match and there are NAC filters defined, then the member tries to send an authentication request to a server in the RADIUS authentication server group.

If you want the member DHCP server to grant leases to specific DHCP ranges when the RADIUS authentication server group is considered disabled (server state = disabled) or if all RADIUS servers are down (server state = failure), create a NAC filter for each situation and apply it to the appropriate range.
Note that when you create a NAC filter, you do not have to include rules that specify prerequisite conditions. For example, when you create a filter that specifies a RADIUS server compliance state or user class, you do not have to include rules that specify the following: server state=success, server response=accept, and server error = no.

Defining NAC Filters

To define a NAC filter:

1. From the Data Management tab, select the DHCP tab -> IPv4 Filters tab, and then expand the Toolbar and click Add -> IPv4 NAC Filter.
   or
   From any panel in the DHCP tab, expand the Toolbar and click Add -> IPv4 NAC Filter.
2. In the Add Filter Wizard, complete the following and click Next:
   - Name: Enter a name for the filter. You can enter a maximum of 255 characters. The name must be unique within a specific network. If you want to specify option settings in the filter, the name must be unique among all NAC filters.
   - Comment: Optionally, enter additional information about the NAC filter.
3. Create a rule as follows:
   - In the first drop-down list, select one of the following criterion: Compliance State, Server Error, Server Response, Server State or User Class.
   - In the second drop-down list, select an operator: equals or does not equal.
   - The selections in the third drop-down list depend on the criterion you selected:
     Compliance State: Select one of the following compliance states: Unknown, Non-compliant, Compliant or Partially Compliant.
     Server Error: The Infoblox DHCP server expects certain RADIUS VSAs in the Access-Accept packet. When any of the VSAs are missing, then the DHCP server considers this an error. For information about the Access-Accept packet and the VSAs, refer to the documentation for the specified RADIUS server. Select one of the following:
       Yes: Create a rule that matches when the RADIUS server sends an Access-Accept packet with a missing VSA.
       No: Create a rule that matches when the RADIUS server sends an Access-Accept packet with no errors.
     Server Response: Select one of the following:
       Accept: Create a rule that matches when the server sends back an Access-Accept packet.
       Reject: Create a rule that matches when the server sends back an Access-Reject packet.
     Server State: Select one of the following:
       Success: Create a rule that matches when at least one RADIUS server in the group is up.
       Fail: Create a rule that matches when the MAC address of the DHCP client is not in the cache and all RADIUS servers in the server group are down.
       Disable: Create a rule that matches when the RADIUS authentication server group is disabled, all servers in the group are disable, or the member was not assigned a server group.
     User Class: Enter the RADIUS user class value, for example, NACDeny. The member DHCP server does not validate the entry. Therefore, you must make sure that the user class you enter matches the user class name on the RADIUS server.
4. Click Next and complete the following to define DHCP options:
   - Option Space: Select an option space from the drop-down list. This field is not displayed if you do not have custom option spaces. The appliance uses the DHCP option space as the default.
   - Lease Time: Enter the value of the lease time in the field and select the time unit from the drop-down list. The lease time applies to hosts that meet the filter criteria.

Options to Merge with Object Options

Click the Add icon. Grid Manager adds a new row to the table with the default DHCP option space and option name displayed. Complete the following:

- Option Space: Click the down arrow and select an option space from the drop-down list. The selected option space contains the corresponding DHCP options.
- Option Name: Click the down arrow and from the drop-down list, select the DHCP option you want to return to the matching client.
- **Value**: Enter the match value that you want the filter to use for the selected DHCP option. For example, enter the value 172.124.3.0 for the SUNW.SrootIP4 option.

To add more options to the filter, click the Add icon and repeat the steps.

5. Click **Next** to define extensible attributes. For information, see *Using Extensible Attributes*.

6. Save the configuration and click **Restart** if it appears at the top of the screen.

After you add NAC filters, you must then apply them to DHCP ranges, as described in *Applying Filters to DHCP Objects*. You can also list, modify or delete NAC filters, as described in *Managing DHCP Filters*.

### Disabling NAC Filters

NAC filters are enabled by default. When you disable them, the appliance bypasses evaluations of all NAC filters for the entire Grid. There are no configuration changes, service restarts, or service down times when you disable the NAC filters. The appliance keeps the filter configurations so you can enable them at a later time.

To disable NAC filters for the Grid:

1. From the **Data Management** tab -> **DHCP** tab, select **Grid DHCP Properties** from the Toolbar.
2. In the **Grid DHCP Properties** editor, click **Toggle Advanced Mode**, select the **General** tab -> **Advanced** tab, and then complete the following in the Common Properties section:
   - **Disable All NAC Filters**: Select this to disable all NAC filters in the Grid. The appliance keeps the filter configurations so you can enable them when needed.

### Chapter 33 Managing Leases

This chapter explains how to manage IPv4 and IPv6 leases. It contains the following sections:

- **About DHCP Leases**
- **Viewing Current Leases**
- **Viewing Detailed Lease Information**
- **Viewing Lease History**
- **Viewing Lease Event Detailed Information**
- **Exporting Lease Records**
- **Clearing Leases**

### About DHCP Leases

Historical DHCP lease records complement the real-time DHCP lease viewer by allowing the appliance to store and correlate DHCP lease information over the lifetime of a lease. You can see critical information such as when the appliance issued or freed an IPv4 or IPv6 address, the MAC address or DUID and host name of the device that received the IP address, the Grid member that supplied the lease, and the start and end dates of the lease.

You can view current leases and lease history in the **Data Management** -> **DHCP** -> **Leases** tab in Grid Manager. To view lease history, you must first enable lease logging at the Grid level. For information, see *Configuring DHCP Logging* and *Configuring the Lease Logging Member*.

You can also export the DHCP lease history log in CSV format for archival and reporting purposes. In the **Leases** tab, you can do the following:

- View current leases. For information, see *Viewing Current Leases*.
- View detailed information about a specific lease. For information, see *Viewing Detailed Lease Information*.
- View historical lease records. For information, see *Viewing Lease History*.
- View detailed information about a lease event. For information, see *Viewing Lease Event Detailed Information*.
- Export current leases and lease history logs. For information, see *Exporting Lease Records*.
- Clear leases. For information, see *Clearing Leases*.

You can also use the filter and **Go to** functions in the lease panels to retrieve lease information for specific hosts, MAC addresses, and IP addresses. These capabilities are crucial for security auditing and for meeting new compliance regulations such as SOX and HIPAA. You can also sort the lease information by column.

### Use case of DHCP service using vNIOS

- The Infoblox vNIOS integrated with a Virtual Machine like VMware can act as a DHCP server and lease IP address to a client virtual machine.
- The on-premises Infoblox NIOS can also act as a DHCP server and lease IP address to a client virtual machine.
Viewing Current Leases

To view current IPv4 and IPv6 leases:

1. From the Data Management tab, select the DHCP tab -> Leases tab -> Current Leases.
2. Grid Manager displays the following information:
   - **IP Address:** The IPv4 address or IPv6 prefix or address that the appliance assigned to a DHCP client for this lease.
   - **Protocol:** Indicates whether the lease is for an IPv4 or IPv6 address.
   - **Members/Servers:** The Grid member or Microsoft server (for IPv4 leases only) that granted the lease.
   - **MAC address:** The MAC address of the IPv4 DHCP client that received the lease for an IPv4 address.
   - **DUID:** The DHCP Unique Identifier (DUID) of the IPv6 DHCP client that received the lease for an IPv6 address.
   - **Host Name:** The hostname that the DHCP client sent with its DHCP request. For IPv4 leases, this field displays the hostname of the DHCP client. For IPv6 leases, this field typically displays the FQDN.
   - **Fingerprint:** The name of the DHCP fingerprint or vendor ID of the DHCP client that was identified through DHCP fingerprint detection. This field displays No Match for devices that do not have any DHCP fingerprint information. For information about DHCP fingerprints, see DHCP Fingerprint Detection.
   - **State:** The binding state of the current lease. The lease state can be one of the following:
     - **Free:** The lease is available for clients to use.
     - **Active:** The lease is currently in use by a DHCP client.
     - **Static:** The lease is a fixed address lease.
     - **Expired:** The lease was in use, but the DHCP client never renewed it, so it is no longer valid.
     - **Abandoned:** The appliance cannot lease this IP address because the appliance received a response when pinging the address.
   - **Start:** The day, date, and time when the state of the lease starts.
   - **End:** The day, date, and time when the state of the lease ends.
   - **Discoverer:** The DHCP client identifier (option 61) in an IPv4 lease. The client sends the client identifier as option 61 in the DHCP DISCOVER and REQUEST packets, as described in RFC2132, DHCP Options and BOOTP Vendor Extensions. The client identifier is either the MAC address of the network interface card requesting the address or any string uniquely identifying the client. This field is not displayed by default.
   - **Username:** Displays the name of the user who receives the lease for the IP address. The username enables you to differentiate between guest users and authenticated users. If you log in as an authenticated user, your username is whatever you choose when you log in. If you log in as a guest, your username is First: first_name Last: last_name. For example, if your first name is John and last name is Doe and your username is jdoe, when you log in as an authenticated user, your username is jdoe. If you log in as a guest user, your username is First: John, Last: Doe.
   - **Client ID:** The DHCP client identifier (option 61) in an IPv4 lease. The client sends the client identifier as option 61 in the DHCP DISCOVER and REQUEST packets, as described in RFC2132, DHCP Options and BOOTP Vendor Extensions. The client identifier is either the MAC address of the network interface card requesting the address or any string uniquely identifying the client. This field is not displayed by default.
   - **OS:** The operating system of the discovered host or virtual entity. The OS can be one of the following:
     - **Microsoft** for all discovered hosts that have a non-null value in the MAC addresses using the NetBIOS discovery method.
     - A value that a TCP discovery returns.
     - The OS of a virtual entity on a vSphere server.
   - **NetBIOS Name:** The name returned in the NetBIOS reply or the name you manually register for the discovered host.
   - **Discovered Name:** The name of the network device associated with the discovered IP address.
   - **Discoverer:** Specifies whether the IP address was discovered by a PortIQ or NIOS discovery process.

**Note:** The dates and timestamps in the Leases tab are determined by the time zone setting of the admin account that you use to log in to the appliance.

You can display the following discovered data for IPv4 leases:
- **Last Discovered:** The timestamp when the IP address was last discovered. This data is read-only.
- **OS:** The operating system of the discovered host or virtual entity. The OS can be one of the following:
  - **Microsoft** for all discovered hosts that have a non-null value in the MAC addresses using the NetBIOS discovery method.
  - A value that a TCP discovery returns.
  - The OS of a virtual entity on a vSphere server.
- **NetBIOS Name:** The name returned in the NetBIOS reply or the name you manually register for the discovered host.
- **Discovered Name:** The name of the network device associated with the discovered IP address.
- **Discoverer:** Specifies whether the IP address was discovered by a PortIQ or NIOS discovery process.

You can do the following in this tab:
- **Sort the data in ascending or descending order by column.**
- **View the lease detailed information of a current lease by selecting the check box of the lease, and then clicking the Open icon.**
- **Change a current lease state to Free by selecting the check box of a current lease, and then clicking the Delete icon.**
- **Use filters and the Go to function to narrow down the list.** With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- **Create a quick filter to save frequently used filter criteria.** For information, see Using Quick Filters.
- **Print and export the data in this tab.**

Viewing Detailed Lease Information

You can view detailed information about a specific lease. To view detailed information of a specific lease:

1. From the Data Management tab, select DHCP tab -> Leases -> Current Leases -> lease check box, and then click the Lease Details icon.
   - or From the Data Management tab, select the IPAM tab, drill down to the IP Map, IP List, or IP address panel, and then click Lease Details from the Toolbar.
2. In the Lease Detailed Information viewer, Grid Manager displays the following for each type of lease:
For IPv4 leases, it displays the fields Member, MAC address, Host, Start, End, Binding State, Username, Binding State, as described in Viewing Current Lease, plus the following information:

- **Lease Issue:** The date and time when the lease was issued. Displayed in the lease event details report only.
- **Event:** The action taken. This can be one of the following: Issued, Renewed, Freed, or Abandoned. Displayed in the lease event details report only.
- **Served by:** The member that provides DHCP services to the lease.
- **Next Binding State:** The subsequent binding state when the current lease expires. The lease state and the next binding state can be one of the following:
  - Free: The lease is available for clients to use.
  - Active: The lease is currently in use by a DHCP client.
  - Static: The lease is a fixed address lease.
  - Expired: The lease was in use, but the DHCP client never renewed it, so it is no longer valid.
  - Released: The DHCP client returned the lease to the appliance.
  - Abandoned: The appliance cannot lease this IP address because the appliance received a response when pinging the address.
- **Billing Class:** The billing class of the lease.
- **Option 82 Agent ID:** The agent ID of the relay agent filter (option 82). A relay agent can append DHCP option 82, relay agent information, to a message that it forwards from a DHCP client to a DHCP server.
- **Option 82 Circuit ID:** The circuit ID of the relay agent filter (option 82).
- **Option 82 Remote ID:** The remote ID of the relay agent filter (option 82).
- **Option 82 Link Selection:** The remote ID of the relay agent filter (option 82).
- **Option 82 Server ID Override:** The remote ID of the relay agent filter (option 82).

**Note:** The agent, circuit, and remote IDs for option 82 can be displayed in hexadecimal or plain text format. By default, Grid Manager displays them in hexadecimal format. You can change the logging format, as described in Defining Logging Format for DHCP Option 82.

For IPv4 leases, it displays the fields for the lease:

- **IP Address:** The IPv4 address or IPv6 prefix or address of the lease.
- **MAC Address:** The MAC address of the IPv4 lease.
- **DUID:** The DUID of the IPv6 DHCP client that received the lease for an IPv6 address.
- **Preferred Lifetime:** The length of time that a valid address is preferred. A preferred address can be used with no restrictions. When this time expires, the address becomes deprecated.

**Viewing Lease History**

To view lease history:

- From the Data Management tab, select the DHCP tab -> Leases tab -> Lease History.

Grid Manager displays a table of historical leases that have been archived in the system. You can export the information in the lease history table. You can also search by the IP address or MAC address of the lease. Grid Manager displays the following read-only information:

- **Lease Issue:** The date and time when the lease was issued.
- **Protocol:** Indicates whether the lease is for an IPv4 or IPv6 address.
- **IP Address:** The IPv4 address or IPv6 prefix or address of the lease.
- **MAC Address:** The MAC address of the IPv4 lease.
- **DUID:** The DUID of the DHCP client that received the lease for an IPv6 address.
- **Fingerprint:** The name of the DHCP fingerprint or vendor ID of the DHCP client that was identified through DHCP fingerprint detection. This field displays No Match for devices that do not have any DHCP fingerprint information. For information about DHCP fingerprints, see DHCP Fingerprint Detection.
- **Host Name:** The host name that the DHCP client sent to the appliance.
- **Action:** This can be one of the following: Issued, Renewed, Freed, or Abandoned.
- **User Name:** The name of the user who received the lease for the IP address.
- **Start:** The start date of the lease.
- **Stop:** The end date of the lease.
- **Member/Server:** The DHCP member or Microsoft server that granted the lease.
- **Member IP Address:** The IP address of the DHCP member that granted the lease. You can do the following in this section:
  - View the lease event detailed information of a historical lease by selecting the check box of a lease, and then clicking the Open icon.
  - Print or export the information in this section.

Copyright ©2019, Infoblox, Inc. All right reserved.
Viewing Lease Event Detailed Information

You can view detailed information about a historical lease record by clicking the lease in the Data Management tab -> DHCP tab -> Leases tab -> Lease History. Grid Manager displays the event, the date and time when the event occurred, plus detailed information about the historical lease record. For information about the fields, see Viewing Detailed Lease Information.
You can also export and print the information in this panel. For information, see Exporting Lease Records.

Exporting Lease Records

The DHCP lease history log holds a maximum of 100,000 entries. After that maximum is reached, the appliance begins deleting entries, starting with the oldest. To archive DHCP lease history logs, you can export them and save them as CSV (comma separated variables) files. You do not need to export the entire log. You can selectively export a section of the log, such as the lease events for a single day.
As a conservative approach to archiving DHCP lease data, Infoblox recommends exporting the log on a daily basis, perhaps through API (application programming interface) scripting. By exporting the daily log entries every day over a certain period of time and then opening the exported files with a spreadsheet program, you can see the number of entries for each day. You can then estimate how often you need to export the log to ensure that you save all of the entries before the log fills up (at 100,000 entries). As a result, you might discover that you need to export the log more or less frequently than once a day to archive all the records.
A limited-access admin group can view and export the DHCP lease history if it has read-only permission to the DHCP lease history. For information on setting permissions for the DHCP lease history, see Administrative Permissions for the IPv4 and IPv6 DHCP Lease Histories. In addition, you can export the displayed DHCP current lease information or you can export them to a CSV file.
To export displayed current lease information:

1. From the Data Management tab, select the DHCP tab -> Leases tab -> Current Leases.
2. Click the Export icon and select Export visible data. For more information on how to export, see Exporting Displayed Data.

To export DHCP current lease information to a CSV file:

1. From the Data Management tab, select the DHCP tab -> Leases tab -> Current Leases.
2. Click the Export icon and select Export data in Infoblox CSV Import format. For more information on how to export, see Exporting Data to Files.

To export a lease history log:

1. From the Data Management tab, select the DHCP tab -> Leases tab -> Current Leases or Lease History.
2. Click the Export icon and select.
3. In the Export dialog box, click Start
4. Click Download when the export is complete. Ensure that you turn off the pop-up blocker in your browser.
5. In the File Download dialog box, select the appropriate action to either open or save the CSV file.

Clearing Leases

You can clear active leases for which you have read/write permission. When you clear an active lease, its IP address becomes available and its status changes to “Free”. To clear an active lease:

1. From the Data Management tab, select the DHCP tab -> Leases tab -> Current Leases.
2. Click the check boxes beside the IP addresses of the leases you want to clear, and then click the Clear Lease icon.

Grid Manager clears the selected leases. You can view information about a cleared lease, by selecting it in the Lease History panel and clicking the Edit icon.

Part 6 Managing Microsoft Windows Servers

This section describes how you can centrally manage Microsoft Windows® DNS and DHCP servers from Grid Manager. You can synchronize your DNS and DHCP data from the Microsoft servers to the Grid, and then use IPAM tools to facilitate DHCP and DNS configuration and data management. This section includes the following chapters:

- Chapter 34, Managing Microsoft Windows Servers
- Chapter 35, Managing Microsoft DNS Services
- Chapter 36, Managing Microsoft DHCP Services

Chapter 34 Managing Microsoft Windows Servers

This chapter explains how to configure Grid members to manage Microsoft Windows DNS and DHCP servers from Grid Manager. It includes the following sections:
About Managing Microsoft Servers

Requirements
Deployment Guidelines
Limitations for Scheduling Full Upgrades

Configuring Members to Manage Microsoft Servers
• Setting Microsoft Server Credentials
• Configuring a Managing Member

Configuring Grid Properties for Managing Microsoft Servers
• Defining Monitor and Control Settings for DNS and DHCP Services
• Synchronizing DNS Reporting Data
• Output Destination for Log Messages
• Maximum Simultaneous Connections for Microsoft Servers
• Configuring RPC Timeout Settings
• Setting Grid Properties for Managing Microsoft Servers
• Forwarding WINS Packets to Microsoft Servers

Managing Microsoft Servers
• Setting Microsoft Server Properties
• Changing the Managing Member or Management Mode
• Backing Up Synchronized Data
• Disabling Synchronization
• Removing a Managed Microsoft Server

About Active Directory Sites and Services
• Best Practices for Configuring Active Directory Sites and Services
• Configuring and Managing Server Permissions

Configuring Active Directory Sites and Associated Networks

Managing Active Directory Sites
• Viewing Active Directory Domains and Sites
• Modifying Active Directory Sites and Networks
• Deleting Active Directory Sites
• Moving Networks Between Active Directory Sites
• Associating Active Directory Sites with Networks
• Configuring Microsoft Server and LDAP Connections
• Configuring Server Site Links

Managing Active Directory Sites and Associated Networks
• Managing an Active Directory Site from the Microsoft server
• Managing an Active Directory Site from NIOS
• Managing Network Operations from Microsoft server
• Managing Network Operations from NIOS
• Restoring Server Data

Configuring Identity Mapping
• Administrative Permissions
• About User Sessions
• Login and Logout Timestamps

Monitoring Managed Microsoft Servers
• Viewing DNS and DHCP Service Status on Microsoft Servers
• Viewing Detailed Status Information
• Viewing Synchronization Logs

About Managing Microsoft Servers

You can configure Grid members to manage Microsoft Windows DNS and DHCP servers, and synchronize their DNS and DHCP data to the Grid database, so you can view and optionally, manage the data from Grid Manager. After the data is synchronized, you can use the IPAM tools of Grid Manager to simplify DNS and DHCP configuration and troubleshooting. You can use Smart Folders to organize your data, and monitor your networks and Microsoft servers from the Dashboard. In addition, you can control the DNS and DHCP services of the Microsoft servers from Grid Manager and configure server properties as well. You can use the Identity Mapping feature to get visibility of user interaction with their environments. For more information about the Identity Mapping feature, see Configuring Identity Mapping.

Figure 34.1 illustrates a Grid that includes a member that provides DNS and DHCP services, and two other members that manage multiple Microsoft DNS and DHCP servers. Assuming the admin has the appropriate permissions, the admin can centrally manage the Microsoft DNS and DHCP servers and Infoblox DNS and DHCP server from a single interface, Grid Manager.

Figure 34.1 Managing Microsoft and Infoblox DNS and DHCP Servers from the Grid Master
You do not have to configure or install any application on the Microsoft servers for the Grid members to communicate with the servers. Infoblox uses MS-RPC (Microsoft Remote Procedure Calls) to manage Microsoft servers.

A Grid member can manage a Microsoft server in either of two modes, Read-only or Read/Write. In Read-only mode, the Grid member synchronizes data from the Microsoft server to the Grid so admins can use Grid Manager to view the synchronized data, but not update it. Read/Write mode allows admins to update the synchronized data as well.

Updates from Grid Manager are then synchronized to the Microsoft server, and updates from the Microsoft server are synchronized to the Grid. Configuration changes and data synchronized from the Grid to the Microsoft server apply immediately after the synchronization. You do not have to restart the Microsoft server or for DNS, reload the zones.

Note that due to a field length limit set on the Microsoft DHCP server, after you synchronize DHCP data on the Microsoft server, the "Comment" and "Description" fields for a fixed address and reservation can display only up to 128 characters even though NIOS allows up to 256 characters for these fields.

Requirements

A Grid member must have a Microsoft Management license installed to manage a Microsoft server. The license allows the member to synchronize data with Microsoft servers. It also activates the tabs, dialog boxes and other elements in Grid Manager that you need to manage a Microsoft server.

Note that if you do not see the Microsoft Servers tab after you add a member that has a Microsoft Management license, you might have to restart the Grid Master to view the tab and to manage Microsoft DNS and DHCP servers in the Grid.

Supported Windows Versions

Infoblox Grid members can manage Microsoft servers that support the following Windows versions:

<table>
<thead>
<tr>
<th>OS</th>
<th>Levels</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 2003 Standard and Datacenter</td>
<td>SP2</td>
<td>32 bits</td>
</tr>
<tr>
<td>Microsoft Windows 2003 R2 Standard and Datacenter</td>
<td>Initial Release</td>
<td>32 bits, 64 bits</td>
</tr>
<tr>
<td>Microsoft Windows 2008 Standard and Datacenter</td>
<td>SP2</td>
<td>32 bits, 64 bits</td>
</tr>
<tr>
<td>Microsoft Windows 2008 R2 Standard and Datacenter</td>
<td>Initial Release</td>
<td>64 bits</td>
</tr>
<tr>
<td>Microsoft Windows 2012 Standard and Datacenter</td>
<td>Initial Release</td>
<td>64 bits</td>
</tr>
<tr>
<td>Microsoft Windows 2012 R2 Standard and Datacenter</td>
<td>Initial Release</td>
<td>64 bits</td>
</tr>
<tr>
<td>Microsoft Windows 2016 Standard and Datacenter</td>
<td>Initial Release</td>
<td>64 bits</td>
</tr>
</tbody>
</table>
Infoblox supports the following SMB (Server Message Block) protocol versions for Microsoft Windows servers: SMB version 1 (SMBv1), SMB version 2.x (SMBv2.x), and SMB version 3.x (SMBv3.x).

Grid members check the Windows version of the Microsoft servers before each synchronization. If a Microsoft server reports an unsupported version before a synchronization, the member logs an error and the synchronization fails.

Note that some Windows versions require certain updates and hotfixes installed, so the Microsoft server can synchronize with the Grid member. Following are the current requirements:

- Windows Server 2003, Enterprise x64 Edition requires the installation of security update 935966.
- Windows Server 2008 R2 requires the hotfix referenced in the Knowledge Base article 981776.
- Windows Server 2008-based DNS servers might not display delegations for reverse lookup zones. For information about this issue, including the available hotfix, refer to Knowledge Base article 958190.

For information about the updates, enter their IDs in the Search field of the Microsoft Support website at http://support.microsoft.com.

Administrative Permissions

By default, only superusers can configure Grid members to manage Microsoft servers. Superusers can give limited-access users Read-only or Read/Write permission to Microsoft servers. Read-only permission allows admins to view the properties and data of a Microsoft server from Grid Manager. Write permission is required to configure Grid members to manage Microsoft servers, edit their properties, and start or stop their DNS and DHCP services. For additional information, see Administrative Permissions for Microsoft Servers.

Note that to view and manage the DNS and DHCP data synchronized from Microsoft servers, admins must have permissions to the applicable DNS and DHCP resources. For example, to view DNS zones synchronized from Microsoft servers, admins must have Read-only permission to edit the zones, admins need Read/Write permission to them. Similarly, to view DHCP ranges synchronized from Microsoft servers, admins must have Read-only permission to edit DHCP ranges, and to edit the DHCP ranges, admins need Read/Write permission to the DHCP ranges. For information, see Administrative Permissions for DNS Resources and Administrative Permissions for DHCP Resources.

The administrative permissions on the Grid are different from those on the Microsoft server. These permissions are independent of each other and are not synchronized.

Deployment Guidelines

Following are some recommendations and considerations when configuring Grid members to manage Microsoft servers:

- Infoblox recommends that you schedule the initial synchronization at a time when your network is less busy, especially if you are synchronizing a large amount of data. In addition, if a Microsoft server reconnects after being disconnected for a long period of time, it could synchronize a significant amount of data and this could impact the Grid Master performance.
- vNIOS Grid members and Grid members running on Infoblox-250, Trinzic 100, and Trinzic 810 appliances do not support being configured as managing members.
- The managing member must be close, in terms of network hops, latency and bandwidth, to the Microsoft servers that it manages. This will help reduce the synchronization time and potential retries due to network delays.
- Although a Grid member that manages Microsoft servers can run other protocols and services, to optimize performance, Infoblox recommends that you configure one or more members solely for managing Microsoft servers.
- Grid members connect to Microsoft servers using RPC calls over TCP/IP. You must adjust your firewall policies to allow traffic between the managing Grid member and its assigned Microsoft servers. Grid members use the VIP as their source port. In Windows Server 2003, RPC uses the dynamic port range 1025-5000, by default. In Windows Server 2008, RPC uses the dynamic port range 49152-65535, by default. You can reduce the number of available ports as follows:
  - In Windows Server 2003, use the rpccfg.exe tool. For information, refer to http://support.microsoft.com/kb/908472.
  - In Windows Server 2008 and later, use the netsh tool. For information, refer to http://support.microsoft.com/kb/929851.

The minimum number of ports required in the range is 255.

Note that TCP ports 135 and 445 must be open on the Microsoft server, in addition to the dynamic port range. Ports 135 and 445 are used by the port mapper interface, which is a service on the Microsoft server that provides information to clients on which port to use to connect to a specific service, such as the service that allows the management of the DNS service.

- The capacity of the managing member must be greater than or equal to the sum of all its assigned Microsoft servers.
- The capacity of the Grid Master must be greater than or equal to the sum of all managed Microsoft servers.
- A Microsoft server can synchronize its data to only one network view, and for DNS data, only one DNS view.
- Multiple Microsoft servers can synchronize their data into the same network view and DNS view, unless there is a conflict in their data. For example, two Microsoft servers in different locations could serve the same private IP address space, such as 10.1.0.0/16, or serve reverse-mapping zones with the same name, such as 10.in-addr.arpa. Synchronizing their data to the same network view and DNS view would cause conflicts which result in the Grid member synchronizing the data of only one Microsoft server and logging an error for the other Microsoft server. In such situations, Infoblox recommends that you synchronize each Microsoft server to a different network view and DNS view to ensure that data from both servers are synchronized.

- This release supports the following Microsoft IPAM enhancements:
  - Monitor and control settings for DNS and DHCP services for Microsoft servers
  - Synchronization of IP addresses with invalid MAC addresses
  - Output destination for Microsoft server log messages in the syslog
  - Synchronization and configuration of Microsoft DHCP failover relationships
  - RPC (Remote Policy Call) timeout setting
  - Maximum concurrent connections for Microsoft servers
  - Enabling and Disabling DNS zone synchronization

Copyright ©2019, Infoblox, Inc. All right reserved.
The ability to allow GSS-TSIG based DDNS updates from multiple clients in a single forest or multiple forests using keys that are appropriate for their respective domains.

Earlier NIOS releases do not support these features. When you modify settings related to these features on Microsoft servers assigned to Grid members running a NIOS release earlier than NIOS 6.11, the NIOS appliance displays an error message.

Limitations for Scheduling Full Upgrades

When you schedule a full upgrade to NIOS 6.11 and later, you can set the RPC (Remote Procedure Calls) timeout settings and maximum concurrent connections immediately on any member as soon as you upgrade the Grid Master. When you disable the synchronization of a DNS zone, NIOS displays an error message if any Microsoft server that is a potential synchronization master, which is assigned to a Grid member, has not been upgraded to NIOS 6.11.0 or later versions.

The following happens if a DHCP failover configuration exists:

- Any Microsoft server configured to manage DHCP and assigned to a Grid member, which has not been upgraded, synchronizes the DHCP configuration without any failover related data.
- You cannot assign a Microsoft server that is assigned to a Grid member, which has not been upgraded, to any Microsoft failover relationship.
- NIOS manages any DHCP scope that is identified to be part of a Microsoft failover relationship but is managed by a Grid member that has not been upgraded, in Read-only mode.

Configuring Members to Manage Microsoft Servers

You can manage Microsoft DNS and DHCP servers on any Grid member. To avoid performance issues, Infoblox strongly recommends that you do not configure Microsoft DNS and DHCP servers on the Grid Master and Grid Master candidate.

When an HA pair manages Microsoft servers, the active node handles synchronization. If an HA failover occurs during a synchronization, the failing node immediately aborts the synchronization. The new active node resumes the next synchronization. Changes that occurred on the Grid since the end of the last synchronization are lost.

For Microsoft DHCP failover, NIOS supports both the hot standby and load sharing modes in both Read/Write and Read-only modes on DHCP servers running Microsoft Windows 2012 and 2012 R2. For more information about Microsoft DHCP failover, refer to the Microsoft documentation.

Complete the following tasks to configure a Grid member to manage a Microsoft server:

1. On the Microsoft server, create a user account for the Grid member. For information, see Setting Microsoft Server Credentials.
2. On the Grid Master, configure the managing member, as described in Configuring a Managing Member.

Setting Microsoft Server Credentials

To enable a Grid member to synchronize data with a Microsoft server and control DNS and DHCP services, you must do the following on the Microsoft server:

1. Create a user account for the Grid member.
2. Grant the user account the necessary permissions.

You can either add the user account to the Administrators Group or add the user account to specific groups and explicitly set only the permissions necessary to access the DHCP and DNS services of the Microsoft server. The following sections provide general instruction on each method.

Adding User Account to the Administrators Group

Adding the user account of the Grid member to the Administrators Group provides total control over the Active Directory Domain. Do one of the following:

- If the managed Microsoft server is a standalone server or a member server in a domain, open Computer Management, click Groups, and add the user account to the Administrators Group.
- If the managed Microsoft server is a domain controller, open Active Directory Users and Computers, select the domain name, click BuildIn, and add the user account to the Administrators Group.

Setting Specific Group Memberships and Permissions

If your security policy precludes adding user accounts to the Administrators group, you can add the user account to individual groups and grant only the required permissions. For guidelines and more information, see the following:

http://support.microsoft.com/kb/325349
http://support.microsoft.com/kb/914392

To add the user account of the Grid member to individual groups and grant specific permissions:

- To enable the member to synchronize DNS data with the Microsoft server, add its user account to the DnsAdmins Group.
- To enable the member to synchronize DHCP data with the Microsoft server, add its user account to the Dhcp Administrators Group.
To enable the Grid member to monitor, start, and stop the DNS and DHCP services, grant the user account permissions on the Service Control Manager (SCM), as follows:


To find additional information, you can also search for “Least Privilege Setup” on the Microsoft sites.

2. Grant permissions to the DNS and/or DHCP service on each managed server by doing one of the following:
   - Use the `sc` command line utility to remotely configure each managed DNS or DHCP server.
     Note that you need to know the SID of the user account and its current permissions. You can retrieve the SID of the user account by using the `dsquery` and `dsget` commands.
   - Use the Domain Controller Policy editor to define a global policy that applies to all DNS or DHCP services running in a domain or on domain controllers. For additional information, refer to [http://support.microsoft.com/kb/324802](http://support.microsoft.com/kb/324802).

### Configuring a Managing Member

When you configure a member to manage Microsoft servers, you must specify the following:

- The management mode of the Microsoft server. For information, see Setting the Management Mode.
- A network view, if there is more than one in the Grid, and a DNS view, if there is more than one in the network view. For information, see Synchronizing to a Network View and DNS View.

For the steps on configuring the managing member, see Assigning Grid Members to Microsoft Servers.

### Setting the Management Mode

A Grid member can manage a Microsoft server in Read-only mode, which is the default, or in read-write mode. In Read-only mode, the Grid member copies the DNS and DHCP data from the Microsoft server to the Grid so Grid Manager admins can view the synchronized data. They cannot update the data, control the DNS and DHCP service of the Microsoft server, or configure any properties.

When you select Read-only mode for Active Directory sites, you can view the sites and networks that are present on the Microsoft server through Grid Manager. Note that you cannot manage the Active Directory sites and networks directly from the Grid, but you can manage an object within the Grid that is associated with a Read-only Active Directory Site or an Active Directory network. The synchronization process is Read-only and you cannot write into the Microsoft server in this mode.

In Read/Write mode, Grid Manager admins are allowed to update the data of the Microsoft server. Therefore during each synchronization, the Grid member applies changes from the Grid to the Microsoft server and vice versa. Read/Write mode also allows admins to control DNS and DHCP services of the Microsoft server and configure some of their properties.

When you select Read/Write mode for Active Directory Sites, you can view and manage the sites and networks that are present on the Microsoft server through Grid Manager. When you update an object that is associated with the Active Directory Site or an Active Directory network, the changes reflect on the Microsoft server.

Note that the management mode of a Microsoft server is separate from the admin permissions that the appliance requires to access the Microsoft servers and DNS and DHCP resources. An admin must still have the applicable permissions to the Microsoft servers and DNS and DHCP resources they want to access. For information on admin permissions, see Administrative Permissions for Microsoft Servers.

### Synchronizing to a Network View and DNS View

A Microsoft server can synchronize its data only to a single network view and a DNS view. Grid Manager automatically assigns Microsoft servers to the default view when a Grid contains only the default network view and DNS view. If a Grid has more than one network view, you must select a network view for the Microsoft server to synchronize its data; and if there are multiple DNS views, you must select a DNS view as well.

You cannot modify the assigned network view or DNS view of a Microsoft server after its data has been synchronized. Instead, you must remove the Microsoft server and then add it again. For information about removing a server, see Removing a Managed Microsoft Server.

Microsoft servers do not support network views and DNS views. Therefore, network view and DNS view properties have no effect on the DNS and DHCP data that are synchronized from Microsoft servers.

### Assigning Grid Members to Microsoft Servers

To configure a Grid member to manage one or more Microsoft servers:

1. **Grid**: From the Grid tab -> **Microsoft Servers** tab -> **Servers** tab, click the Add icon.
   **Standalone appliance**: From the System tab -> **Microsoft Servers** tab -> **Servers** tab, click the Add icon.

2. In the Add Microsoft Server(s) wizard, complete the following:
   - **Which features do you want to configure?**: This section appears only when you have selected the Enable MS AD feature check box for mapping network users. For more information, see Enabling Identity Mapping. You can select multiple options in this section:
     - **Network Users**: Select this check box to enable the Grid member to synchronize user information with the managed Microsoft servers.
- **DNS and DHCP Services**: Select this check box to enable the Grid member to synchronize DNS and DHCP services with the Microsoft servers.
- **Active Directory Sites**: Select this check box to enable the Grid member to synchronize Active Directory sites.

In the **General Settings** section, complete the following:
- **Managing Member**: Click **Select Member** and select the Grid member that manages Microsoft servers. Select **None** if you do not want to associate a Microsoft server with a Grid member.
- **Credentials to Connect to the Microsoft Server(s)**: Enter the login name and password that the appliance uses to connect to the Microsoft servers. These must be the same as those you specified when you created the user account for the Grid member on the Microsoft servers. Note that you must specify the domain name and the user name in the following format: domain_name\user_name.
- **Manage Server(s) in**: Select the management mode, which is either **Read-only** or **Read/Write**. You can choose to manage the DNS and DHCP synchronization services in either **Read-only** or **Read/Write** mode. For more information, see [bookmark2618](#).
- **Minimum Synchronization Interval (min)**: The default synchronization interval is two minutes. This is the time between the completion of one synchronization and the start of a new one. Synchronizing large data sets could take longer than the synchronization interval, causing a delay in the start of the next synchronization. For example, if the synchronization interval is two minutes but a synchronization takes five minutes, the time between the start of the first synchronization and the start of the next one is approximately seven minutes.

**Note**: The synchronization of Microsoft DHCP servers running Microsoft Windows 2012 or later includes the synchronization of DHCP failover relationships. Note that the DNS and DHCP failover synchronization rules do not have an impact on the Microsoft servers running a Windows version that is earlier than 2012.

- **Logging Level**: Select a logging level for the Microsoft server log from the drop-down list: **Low**, **Normal**, **High**, and **Debug**. NIOS logs the messages based on the logging level you set.
  - **Low**: Logs only error messages.
  - **Normal**: Logs warning and error messages.
  - **High**: Logs warning, error and information messages.
  - **Debug**: Logs messages about all events associated with synchronization.
- **See** [Viewing Synchronization Logs](#) for a description of each level.
- **Logging output destination**: From the drop-down list, select an output destination to which the appliance saves log messages for Microsoft servers. When you select **Microsoft Log**, the appliance logs the messages that are generated for the respective Microsoft server in the existing Microsoft log. This is selected by default. For more information, see [Viewing Synchronization Logs](#). When you select **Syslog**, NIOS logs the messages that are generated for the respective Microsoft server in the syslog. For more information about the syslog, see [Viewing the Syslog](#).
- **Synchronize Data into Network View**: This field appears only when there is more than one network view in the Grid. Specify to which network view the data from the Microsoft servers is synchronized.
- **Synchronize DNS Data into DNS View**: This field appears only when there is more than one DNS view in the network view. Specify to which DNS view the data from the Microsoft servers is synchronized.
- **Comment**: You can enter additional information about the servers.
- **Disable Synchronization**: Select this to disable the Microsoft servers. This allows you to preprovision the Microsoft servers and then enable them at a later time.

3. Click **Next**.

**Note**: Depending on your configuration in the **Which features do you want to configure?** section, the **Add Microsoft Server(s)** wizard displays the Microsoft server setting options.

4. Complete the following:

   - If you have selected the **Network Users** check box, complete the following in the **Select your across-server settings for Network Users** page:
     - **Use General credentials (from first page of wizard)**: Select this check box if you want to use the same credentials that you specified for connecting the Microsoft servers.
     - **Credentials for synchronizing Network User service information**: Specify a username and password to synchronize user information from Active Directory domain controllers. The username you specify here must belong to the Domain User group and Event Log Reader group in Microsoft. For information, see [Prerequisites on the Microsoft Server](#).
     - **Use General synchronization interval (from first page of wizard)**: Select this check box to use the same synchronization interval that you specified in the **Minimum Synchronization Interval** for synchronizing the user and device mapping information from the Microsoft Active Directory authentication logs.
     - **Minimum synchronization interval**: The default synchronization interval is two minutes. This is the time between the completion of one synchronization and the start of a new one. Specify an interval to synchronize user information from the Microsoft Active Directory authentication logs.

   - If you have selected the **DNS and DHCP Services** check box, complete the following in the **Select your across-server settings for DNS and DHCP Services** page:
     - **Use General credentials (from first page of wizard)**: Select this check box if you want to use the same credentials that you specified for connecting the Microsoft servers.
     - **Credentials to connect to DNS and DHCP Services**: Specify a username and password to synchronize DNS and DHCP services. You must use the same username and password that you specify here when the appliance prompts for credentials during DNS or DHCP synchronization.
- **Use General synchronization interval (from first page of wizard):** Select this check box to use the same synchronization interval that you specified in the Minimum Synchronization Interval for synchronizing the DNS and DHCP services as well.

- **Minimum Synchronization interval:** The default synchronization interval is two minutes. This is the time between the completion of one synchronization and the start of a new one. Specify an interval to synchronize the DNS and DHCP data from the Microsoft server.

- **Manage DNS and DHCP services in:** Select a value from the drop-down list. You can choose to manage the DNS and DHCP synchronization services in either Read-only or Read/Write mode. For more information, see bookmark2618.

- **If you have selected the Active Directory Sites check box,** complete the following in the Select your across-server settings for Active Directory Sites page:
  - **Use General credentials (from first page of wizard):** Select this check box if you want to use the same credentials that you specified for connecting the Microsoft servers. Clear the check box to specify a new username and password for managing Active Directory sites.
  - **Credentials for synchronizing Active Directory information:** Specify a username and password to synchronize Active Directory sites. You must specify the same username and password that you specify here when the appliance prompts for credentials while synchronizing Active Directory sites.
  - **Use General synchronization interval (from first page of wizard):** Select this check box to use the same synchronization interval that you specified in the Minimum Synchronization Interval for synchronizing Active Directory sites.
  - **Minimum Synchronization interval:** The default synchronization interval is two minutes. This is the time between the completion of one synchronization and the start of a new one. Specify an interval to synchronize the Active Directory sites.
  - **Manage Active Directory sites in:** Select a value from the drop-down list. You can choose to manage the Active Directory Site in either Read-only or Read/Write mode. For more information, see bookmark2618.
  - **Encryption:** You can encrypt the network traffic between the Grid member and the managed Microsoft server using SSL. Select a value, None or SSL, from the drop-down list. Infoblox strongly recommends that you select SSL from the drop-down list to ensure the security of all communications between the NIOS appliance and the Active Directory server. When you select SSL, the appliance automatically updates the TCP port to 636. When you select this option, you must specify the FQDN of the Microsoft server instead of the IP address and you must upload a CA certificate from the Active Directory server. Click CA Certificates to upload the certificate. In the CA Certificates dialog box, click the Add icon, and then navigate to the certificate to upload it.
  - **TCP port for LDAP connections:** The appliance displays the port number by default based on the encryption type that you select. When you select None, the appliance automatically updates the TCP port to 389.

5. Click **Next** and do the following in the Managed Servers table:

- **Name or IP Address:** Enter either the FQDN or IP address of the Microsoft server. In order for the member to resolve the FQDN of a Microsoft server, you must define a DNS resolver for the Grid member in the DNS Resolver tab of the Member Properties editor. Note that if the IP address of the Microsoft server is specified, then the DNS resolver must resolve it when the member and Microsoft server synchronize DHCP data only.

- **DNS Sync:** Select this option to enable the Grid member to manage the DNS service and synchronize DNS data with this server. Clearing this check box disables DNS service management and data synchronization. This allows you to pre-provision specific Microsoft servers and then enable them at a later time.

- **DHCP Sync:** Select this option to manage the DHCP service of the Microsoft server and synchronize DHCP data with this server. Clearing this check box disables DHCP service management and data synchronization. This allows you to pre-provision specific Microsoft servers and then enable them at a later time.

- **Active Directory Sites:** Select this option to manage Active Directory sites and synchronize Active Directory Sites and networks with the Grid.

- **DNS Monitor & Control:** Click **Override** to override the settings inherited from the Grid. To inherit the same settings as the Grid, click **Inherit**. Select this to enable monitoring and the ability to control DNS service for the Microsoft server. For more information, see Setting Grid Properties for Managing Microsoft Servers.

- **Synchronize DNS Reporting Data:** Click **Override** to override the settings that are inherited from the Grid. To retain the same settings as the Grid, click **Inherit**. Select this to synchronize DNS reporting data from the Microsoft server. For more information, see Synchronizing DNS Reporting Data.

Note that synchronization of DNS reporting data is effective only when DNS Sync option is enabled for the Microsoft server.

- **DHCP Monitor & Control:** Click **Override** to override the setting inherited from the Grid. To inherit the same settings as the Grid, click **Inherit**. Select this to monitor and control DHCP service for the Microsoft server. For more information, see Setting Grid Properties for Managing Microsoft Servers.

**Note:** You cannot start or stop a DNS or DHCP service on a specific Microsoft server if you disable the monitor and control setting for the respective service. You can control and monitor DNS and DHCP services at the Grid level and override the settings at the Microsoft server level. Each monitor and control setting applies only to the DNS or DHCP service and the respective Microsoft server.

- **Synchronize Network Users:** Click **Override** to override the settings inherited from the Grid. To inherit the same settings as the Grid, click **Inherit**. Select this to enable the identity mapping for the Microsoft server. For information, see Enabling Identity Mapping.

You can assign multiple Microsoft servers to a Grid member and test their connection to the Grid member. Click the Add icon to add another Microsoft server.

6. Select a Microsoft server and click the Test Microsoft Server icon, or click the Action icon.
next to the respective Microsoft server and select Test Microsoft Server from the menu to verify whether the appliance can successfully connect to the Microsoft server. The appliance displays the test results in the Test Microsoft Server Results dialog box.

7. Save the configuration and click Restart if it appears at the top of the screen.

or

Click Next: Continue to the next step and define extensible attributes for the Microsoft servers. For information, see Using Extensible Attributes.

After you configure a Grid member to manage a Microsoft server, the member automatically connects to the Microsoft server and starts synchronizing data. You can then do the following:

- View the status of the servers in the Microsoft Servers panel, as described in Monitoring Managed Microsoft Servers. Newly added servers first display a status of Connecting as the Grid member contacts the Microsoft servers. The status changes to OK after the Grid member successfully connects to the Microsoft server.
- View the data synchronized from the Microsoft servers. To view DNS data, navigate to the DNS view you specified. For information, see Viewing Zones. To view DHCP data, navigate to the Networks tab of the network view that you specified. For information, see Managing IPv4 DHCP Data.
- Network conditions and the amount of data can affect the synchronization time. Therefore, you might not be able to view all of the synchronized data immediately.
- Use Smart Folders to organize the Microsoft servers and their data. For example, you can create a folder for DNS zones and another folder for DHCP scopes synchronized from a Microsoft server. For information about Smart Folders, see Chapter 3, Smart Folders.
- Update the synchronized data. For information, see Chapter 35, Managing Microsoft DNS Services, and Chapter 36, Managing Microsoft DHCP Services.

You can also use Global Search to search for synchronized data, such as zones and IP addresses. For information, see Global Search.

Configuring Grid Properties for Managing Microsoft Servers

You can configure the following Grid properties for Microsoft servers that are managed by a Grid member:

- Monitor and control settings for DNS and DHCP services. For information, see 5800342 5800342
- Use the identity mapping feature to get visibility of user interaction with their environments. For information, see Configuring Identity Mapping.
- Output destination for Microsoft server log messages. For information, see 5800342.
- Simultaneous connections for Microsoft servers. For information, see 5800342 5800342.
- Maximum connection timeout setting. For information, see 5800342.
- Forward WINS packets to dedicated Microsoft Windows DNS and DHCP servers. For information see 5800342 5800342.

For more information about configuring other Grid properties for Microsoft servers, see 5800342 5800342.

Defining Monitor and Control Settings for DNS and DHCP Services

You can enable or disable monitor and control settings of DNS and DHCP services for a specific Microsoft server. The appliance enables this by default when you add a Microsoft server. When you upgrade the existing Microsoft servers, the managed member inherits values from the Grid. You can monitor and control the DNS and DHCP services on a Microsoft service only if both the management setting of the respective service and the monitor and control settings of the corresponding Microsoft server for the selected service are enabled. To know more about how to enable monitor and control settings, see 5800342.

Note: The original setting that controls the overall management of a given service is referred to as the management setting. It controls whether the synchronization of the corresponding service is enabled or not, with no change to the existing synchronization behavior. Note that synchronization does not depend on the value of the monitor and control setting for the Microsoft server.

You can configure Microsoft server settings at the Grid level. Note that Microsoft servers inherit these settings by default, and you can override these settings at the Microsoft server level.

When you enable monitor and control settings for DNS and DHCP services, the managing member verifies the corresponding service status on the Microsoft server every 30 seconds. The Grid Master is notified of the status through Grid replication.

When you disable monitor and control setting for DNS and DHCP services, the managing member stops verifying the service status. NIOS administrators cannot start or stop DNS or DHCP service on the Microsoft server. When you try to start or stop these services through the Infoblox API, the appliance generates an error message. The pending service control requests made before disabling the monitor and control settings are sent to the Microsoft server.

For information about the displayed status, see Viewing DNS and DHCP Service Status on Microsoft Servers.
Synchronizing DNS Reporting Data

You can enable synchronization of DNS reporting data from the Microsoft server and view both NIOS and Microsoft services data in a single view in the supported DNS reports. This feature is enabled by default when you add a Microsoft server to the Grid. This feature is supported for Microsoft Windows 2012 R2 and Microsoft Windows 2016 versions, and you must disable this feature for all previous versions of Microsoft Windows servers. When you upgrade the Grid to NIOS 8.2 or later, this feature is disabled. For information about how to enable synchronization of DNS reporting data, see Setting Grid Properties for Managing Microsoft Servers.

You can enable the synchronization of DNS reporting data at the Grid level. The Microsoft servers inherit these settings by default, and you can override these settings at the Microsoft server level. The synchronization of DNS reporting data is effective only if a valid Reporting license is installed on the Grid and when DNS Sync is enabled for the Microsoft server to synchronize the DNS data. For information about how to enable DNS Sync, see Assigning Grid Members to Microsoft Servers.

Note: You must enable DNS logging feature on the Microsoft server for this feature to function properly. To enable DNS logging feature on Microsoft servers, refer to https://technet.microsoft.com/en-us/library/dn800669#some.

When you enable the synchronization of DNS reporting data, the appliance performs the reporting data synchronization from the Microsoft server based on the specified time interval. The default synchronization interval is 15 seconds. You can change the synchronization interval using the CLI command set ms_dns_reports_sync_interval. For information, refer to the Infoblox CLI Guide. The collection of reporting data is dependent on the synchronization intervals set for the Microsoft server. Hence, there would be differences in the Microsoft services data updated in the reports as compared to the NIOS reporting data. Note that only events that are logged in the Microsoft event log are displayed in the Microsoft DNS reports. For a list of DNS reports that display data from both NIOS and the Microsoft server when this feature is enabled, see Reports with Data Synchronized from Microsoft Servers.

Microsoft provides enhanced DNS logging and diagnostics for Microsoft Windows server 2012 R2 and later versions. This includes DNS analytic events logging which enables activity tracking on the DNS server. An analytic event is logged each time the server sends or receives DNS information. In order to install enhanced DNS logging and diagnostics feature in Microsoft Windows server 2012 R2 and later versions, you must apply the query logging and change auditing hotfix. Click the following link to apply the query logging and change auditing hotfix: https://support.microsoft.com/en-us/help/2958577/update-adds-query-logging-and-change-auditing-to-windows-dns-servers.

Note that DNS analytic events logging is not enabled by default on Microsoft servers. To install and enable DNS analytic events logging feature on Microsoft servers, refer to https://technet.microsoft.com/en-us/library/dn800669#some.

Output Destination for Log Messages

You can configure an output destination for Microsoft server log messages at the Grid level and override it at the Microsoft server level. You can choose to save log messages related to Microsoft synchronization in the syslog or Microsoft log. For information, see Viewing the Syslog.

When you change the setting, the Grid Master notifies the managing member about the new setting through Grid replication and sends log messages to the selected destination. The new setting takes effect for synchronization only after the managing member is notified. The synchronization, which is already in progress continues to log messages to the destination based on the old setting. To know more about how to select output destination for log messages, see 5800342.

Maximum Simultaneous Connections for Microsoft Servers

You can specify a maximum number of simultaneous RPC connections that can be configured for the respective Microsoft server, which are managed by the Grid. You can override this value at the Microsoft server level. To know more about how to define maximum simultaneous connections for Microsoft servers, see 5800342 5800342.

Note: When you increase the maximum number of simultaneous connections above the recommended setting for a given Microsoft server, it may consume additional bandwidth, memory, and CPU usage.

Configuring RPC Timeout Settings

You can specify an RPC (Remote Procedure Call) timeout value to control network connectivity for Microsoft servers. You can configure an RPC timeout value at the Grid level and override it for each Microsoft server. The default value at the Grid level is ten seconds and the member inherits this value from the Grid. You can specify a value between one and 60 seconds. To know more about how to configure RPC timeout settings, see 5800342 5800342.

Setting Grid Properties for Managing Microsoft Servers

To configure Grid properties for managing Microsoft servers, complete the following:

1. **Grid:** From the Grid tab -> Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit. Select Microsoft Sync Settings tab in the Grid Properties Editor wizard.

Copyright ©2019, Infoblox, Inc. All right reserved.
**Microsoft Server**: From the Grid tab -> Microsoft Servers tab -> Servers tab, select a Microsoft server and click the Edit icon, or click the Action icon next to the respective Microsoft server and select Edit from the menu. In the Microsoft server editor, click the General tab.

**Standalone appliance**: From the System tab -> System Manager tab, expand the Toolbar and click System Properties -> Edit.

2. Complete the following in the Basic tab:
   - **Logging output destination**: From the drop-down list, select an output destination to which the appliance saves log messages for Microsoft servers. When you select Microsoft Log, the appliance logs the messages that are generated for the respective Microsoft server in the existing Microsoft log. This is selected by default. For more information, see Viewing Synchronization Logs.
   - **Monitor DNS and DHCP Services**: You can enable monitoring and control services for DNS and DHCP services at the Grid level and override the settings for each service at the Microsoft server level. This is enabled, by default. Each monitoring and control setting applies only to the corresponding service and is applicable to the respective Microsoft server only.
     - **Monitor and control DNS Services**: Select this to enable monitoring and the ability to control DNS service for the Microsoft server.
     - **Synchronize DNS Reporting Data**: Select this to synchronize DNS reporting data from the Microsoft server. Clearing this check box disables DNS reporting data synchronization.
     - **Monitor and control DHCP Services**: Select this to enable monitoring and the ability to control a DHCP service for the Microsoft server.

3. Optionally, select the Microsoft Server Settings tab in the Grid Properties Editor wizard and complete the following in the Advanced tab:
   - **Maximum simultaneous connections**: Specify a maximum number of simultaneous RPC connections that can be configured for the respective Microsoft server, which are managed by the Grid. The default is five. You can specify a value between two and 40.
     - You can click Override at the member level to specify a new value. The Override button changes to Inherit. Click Inherit to inherit the value from the Grid.
   - **RPC timeout**: Specify the RPC timeout value in seconds to control the network communication timeout. The default is ten seconds. You can specify a value between one and 60.
     - You can click Override at the member level to specify a new value. The Override button changes to Inherit. Click Inherit to inherit the value from the Grid.

4. Save the configuration.

### Forwarding WINS Packets to Microsoft Servers

If your Infoblox Grid includes legacy Microsoft DNS and DHCP servers, you can configure NIOS to forward WINS packets to dedicated Microsoft servers. Infoblox provides the set wins_forwarding and show wins_forwarding CLI commands you can use to perform this task. For detailed information about these commands, refer to the Infoblox CLI Guide.

When you enable port redundancy in NIOS, the LAN1 and LAN2 ports are grouped into one logical interface. They share one IP address and appear as one interface to the network. If a link to one of the ports fails or is disabled, the appliance fails over to the other port, avoiding a service disruption. When you enable port redundancy, WINS packet forwarding is not supported on the LAN2 interface. You must use the LAN1 interface.

**Note**: Ensure that port 137 is not used for any services in your Grid; otherwise you will not be able to configure the appliance to forward WINS packets to Microsoft DNS and DHCP servers. Likewise, if you have enabled this feature, you will not be able to configure port 137 for any other services in your Grid.

### Managing Microsoft Servers

After you configure Grid members to manage Microsoft servers, you can set certain properties and manage the servers as follows:

- Set server properties, as described in 5800345.
- Change the managing member or the management mode, as described in 5800345 5800345
- Back up the synchronized data, as described in 5800345.
- Disable synchronization with a Microsoft server, as described in 5800345.
- Remove a Microsoft server, as described in 5800345.

### Setting Microsoft Server Properties

You can modify any of the Microsoft server properties you previously configured, except for the network view and DNS view. You can also set certain properties, including the logging level, extensible attributes, and administrative permissions. Extensible attributes and permissions apply to the data only when they are managed from Grid Manager. Extensible attributes and permissions are not synchronized to the Microsoft server.

To set the properties of a Microsoft server:

1. From the Grid tab, select the Microsoft Servers tab -> Servers tab, select a Microsoft server and click the Edit icon, or click the Action
1. In the **Microsoft Server Properties** editor, you can set properties in the following tabs:
   - **General**: Modify the settings described in [Assigning Grid Members to Microsoft Servers](#).
   - **Services (DNS/DHCP)**: Modify DNS and DHCP synchronization settings. For more information, see [Assigning Grid Members to Microsoft Servers](#).
   - **Active Directory Domain/sites**: Modify Active Directory Site settings. For more information, see [Assigning Grid Members to Microsoft Servers](#).
   - **Extensible Attributes**: Define extensible attributes for the server. For information, see [Using Extensible Attributes](#).
   - **Permissions**: Define administrative permissions that apply to the server. For information see [About Administrative Permissions](#).

2. Save the configuration and click **Restart** if it appears at the top of the screen.

---

### Changing the Managing Member or Management Mode

You can change the managing member and the management mode of a Microsoft server.

If you change the managing member, the previous member aborts any ongoing synchronization, and the newly assigned member resumes the synchronization process.

Note that if you switch the managing member or change the management mode of a Microsoft server from Read/Write to Read-only, the Grid member reverts any changes that were made from Grid Manager since the last synchronization. For example, an admin adds a network and DHCP range for a scope. If another admin changes the management mode of the Microsoft server to Read-only before the next synchronization, the Grid member deletes the network and DHCP range at the next synchronization.

To change the member or management mode:

1. From the **Grid** tab, select the **Microsoft Servers** tab -> **Servers** tab, select a Microsoft server and click the Edit icon, or click the Action icon next to the respective Microsoft server and select **Edit** from the menu.

2. In the **Microsoft Server Properties** editor, select the **General** tab and do any of the following:
   - **Managing Member**: Click Select Member and select another Grid member.
   - **Manage Server(s) in**: Select either **Read-only** or **Read/Write**.
3. Save the configuration and click **Restart** if it appears at the top of the screen.

---

### Backing Up Synchronized Data

When you back up the Grid, it includes all managed Microsoft data. If you restore a backup, the data is restored on the Grid only. It is not synchronized to the Microsoft servers. When the Grid member synchronizes the data after the restore operation, it overrides the data on the Grid with the data from the Microsoft servers. For information about backing up and restoring data, see [Chapter 10, Managing NIOS Software and Configuration Files](#).

---

### Disabling Synchronization

When you set the disable option, the Grid member completes any ongoing synchronization and does not start a new one. Setting this option only affects data synchronization and does not affect the operations of the Microsoft server. Synchronization resumes when the Microsoft server is re-enabled.

To disable a Microsoft server:

1. From the **Grid** tab, select the **Microsoft Servers** tab -> **Servers** tab, select a Microsoft server and click the Edit icon, or click the Action icon next to the respective Microsoft server and select **Edit** from the menu.

2. In the **General** tab, select the **Disable Synchronization** option.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

---

### Removing a Managed Microsoft Server

When you remove a Microsoft server from the Grid, the managing member stops any ongoing synchronization and does not start a new one. If the Microsoft server served DNS, the synchronized DNS data remains unchanged in the Grid. If the Microsoft server served DHCP, then Grid
Manager deletes all the DHCP ranges, leases, and fixed addresses associated with the server. It also deletes networks that were assigned only to the Microsoft server. It does not delete a network if it was assigned to other Microsoft servers as well.

Removing a managed Microsoft server from the Grid does not affect the operations of the Microsoft server.

To remove a managed server:

1. From the Grid tab, select the Microsoft Servers tab -> Servers tab, select a Microsoft server and click the Delete icon, or click the Action icon next to the respective Microsoft server and select Delete from the menu.
2. When the Delete Confirmation dialog box appears, click Yes.

For information about how removing a Microsoft server affects the synchronized DNS and DHCP data, see Disabling and Removing Microsoft DNS Servers and Disabling and Removing Microsoft DHCP Servers.

About Active Directory Sites and Services

An Active Directory Site represents physical or logical sites that are defined on a Microsoft server. Each Active Directory Site is associated with an Active Directory Domain. A Microsoft administrator can associate multiple sites and networks with an Active Directory Domain. You cannot associate the same network with multiple Active Directory Sites. For more information about adding an Active Directory Site, see Monitoring Managed Microsoft Servers.

You can synchronize Active Directory Sites, along with the associated networks, from the Active Directory server. The networks that synchronize from the Active Directory server appears in NIOS as a network or a network container. The Active Directory Site to which the network belongs is displayed as an extensible attribute and associated with the respective network. For more information, see Managing Extensible Attributes and Associated Networks. When you create a new Active Directory Site on NIOS, the appliance synchronizes new Active Directory Sites and associated networks with the Active Directory server.

The appliance uses LDAP to communicate with the Microsoft server. For more information, see Configuring Microsoft Server and LDAP Connections. You can specify a site link for a given Active Directory Site. For more information, see Configuring Server Site Links.

You can assign relevant permissions for Active Directory Domains at the Grid level, network view level, or at the object level. For more information, see 4819967.


Best Practices for Configuring Active Directory Sites and Services

- A Grid member configured to synchronize Active Directory Sites and networks of a Microsoft server uses system resources, CPU, memory, network, etc. The amount of consumed resources depends on the number of Microsoft servers that are managed by the Grid member, the amount of data for synchronization and the synchronization frequency. Infoblox recommends that the managing Grid member should not serve other protocols.
- The Grid Master might also be affected by the initial synchronization. The first synchronization replicates all Active Directory Sites and networks from the managing Grid member to the Grid Master.
- The Grid member always initiates the connection to the Microsoft server. Infoblox recommends that you use an encrypted LDAP connection between the Grid member and the Microsoft server. The appliance displays a warning message when you use a non-encrypted connection.
- During a scheduled full upgrade, the synchronization of a Microsoft server is deactivated until the managing Grid member completes its upgrade.
- Microsoft Windows 2003 does not support IPv6 networks. Hence, the appliance prevents you from performing the following operations on the NIOS appliance, which might result in a synchronization failure on the Microsoft server:
  - Assigning an Active Directory Site to an IPv6 network if the site belongs to an Active Directory Domain that is managed by a Windows 2003 server.
  - Creating an IPv6 network from an IPv6 network template in which an Active Directory Site belonging to an Active Directory Domain managed by a Windows 2003 server is defined.
  - Moving one or more IPv6 networks when the destination Active Directory Site belongs to an Active Directory Domain that is managed by a Windows 2003 server.

Synchronizing Active Directory Domains on a Domain Controller

The top level container in the Active Directory is called a Forest. Each forest can contain one or more Active Directory domains. All these domains share the same sites and networks.

To avoid any inconsistency within NIOS, the appliance synchronizes only the root Active Directory domain of the forest into the Grid. For example, if the Microsoft server points to a domain controller of xyz.abc.com domain, the appliance synchronizes abc.com domain in NIOS.

Configuring and Managing Server Permissions

You can define permissions for Active Directory Sites on both the NIOS and Microsoft servers, but there is no relationship between these two sets of permissions and they are not synchronized. You must have relevant permissions on the Microsoft server to synchronize an Active Directory server. If you do not have permissions, the operation fails and the appliance logs the message into the Microsoft log. The synchronization process
fails until appropriate permissions are granted.

On the Active Directory Sites, make sure that you set the following permissions in the Permission Entry for Sites dialog box:

- In the Permissions section, select all the check boxes.
- In the Properties section, select the Read All Properties and Write All Properties check boxes.

An administrator can define relevant permissions on the Active Directory Site and associated networks to prevent them from accidental deletion. However, you can modify such Active Directory Sites and networks. For example, you can rename an Active Directory Site.

You can define permissions for an Active Directory Domain at the following levels:

- Grid level: When you assign Grid level permission, it is applicable to the objects that are associated with the Active Directory Domains that you have defined. When you assign Grid permissions, you can assign either Read/Write, Read-only, or Deny permissions for All Active Directory Domains resource. For more information about how to define Grid level permission, see Defining Grid Permissions.
- Network view level: When you assign permission at the network view level, the permission is applicable to all the Active Directory Domains within the selected network view. For more information, see Administrative Permissions for Network Views.
- Permission on the Active Directory Domain. For more information, see Defining Object Permissions.

You must have the following permissions on the Active Directory Domain to perform the relevant operations:

- Read-only permission on the Active Directory Domain to view the Active Directory Domain and associated Sites.
- Read/Write permission on the Active Directory Domain to add, update or delete an associated Active Directory Site.
- Read/Write permission on the Active Directory Domain to associate or dissociate an Active Directory Site from or to the network.
- Note that the All Active Directory Domains permission will only support two modes: Read-Only and Read/Write. If you do not define permissions explicitly, the appliance sets Read-only permission for Active Directory Domains and Sites.
- Note that the extensible attributes are used to represent Active Directory Domains and Sites. As extensible attributes are generic and they do not support permissions, you can always retrieve Active Directory Domains and Sites for a given network if you have Read-only permission.

Configuring Active Directory Sites and Associated Networks

An Active Directory Domain is a collection of Active Directory Sites and associated networks. Each Active Directory Site can have multiple networks associated with it. The synchronization process ignores a network which is not assigned to an Active Directory Site. You can create and modify Active Directory Sites and networks on the NIOS appliance.

You can use Active Directory Sites and services to synchronize sites and networks from the Active Directory server. After synchronization, the appliance displays these as networks or network containers in the appliance.

The Active Directory Sites that are associated with a network are displayed as extensible attributes, which is a combination of the Active Directory Domain and Site name, for the respective networks on the appliance.

To add Active Directory Sites, you must have Read/Write permission on the respective Active Directory Domain with which it is associated. For more information about permissions, see Configuring and Managing Server Permissions.

To create Active Directory Sites and associate networks:

1. From the Grid tab, select the Microsoft Servers tab -> Active Directory Domains tab and click the respective Active Directory Domain name.
2. Click the Add icon in the New Active Directory Sites wizard and specify a name for the Active Directory Site. You can associate multiple sites with an Active Directory Domain.

Note: You can specify a name up to 63 bytes and it is not case-sensitive, but it cannot contain spaces and the following special characters: | { } ~

You can select an Active Directory Site and click the Delete icon to delete it.

3. Click Next to associate networks with an Active Directory Site. Select an Active Directory Site and click the Add icon to associate networks with the respective site.

4. Click Cancel to close the wizard without saving your settings. You can click Save and Close to save the settings and close the wizard or click Save and Edit to save the settings and edit the properties. The application will close the wizard and open the Active Directory Site Properties editor. Click Save and New to save the Active Directory Sites in the list and open a new wizard.

Managing Active Directory Sites

You can manage Active Directory Sites and networks that you defined earlier and modify their information. You can do the following:

- View Active Directory Domains and sites, as described in Viewing Active Directory Domains and Sites.
- Modify Active Directory Sites and networks, as described in Monitoring Managed Microsoft Servers.
- Delete Active Directory Sites. For more information, see Associating Active Directory Sites with Networks.
• Move networks that are associated with an Active Directory Site to another. For more information, see Moving Networks Between Active Directory Sites.

Viewing Active Directory Domains and Sites

You can view Active Directory Domains that are associated with the Microsoft server. You can also view Active Directory Sites and networks that are associated with the Active Directory Domains.

To view Active Directory Domains and sites:

1. From the Grid tab, select the Microsoft Servers tab -> Active Directory Domains tab.
2. Grid Manager displays the following information:
   - **Name**: The name of the Active Directory Domain. You can click the name to view the Active Directory Sites below it.
   - **NetBIOS Name**: The name returned in the NetBIOS format.
   - **MS Sync Server**: The Microsoft synchronization server that is associated with the Active Directory Domain.
   - **Network View**: The network view that is associated with the Active Directory Domain.

   You can do the following in the Active Directory Domains tab:
   - Sort the Active Directory Domains in ascending or descending order by column.
   - Use filters and the search function to look for specific values.
   - Export and print the information in the table.

3. To view Active Directory Sites associated with an Active Directory Domain, click the domain name that is displayed as a hyperlink. The appliance displays the list of Active Directory Sites that are associated with the respective Active Directory Domain in the Active Directory Domains Home table.

   You can do the following in the Active Directory Domains Home table:
   - Sort the Active Directory Sites in ascending or descending order by column.
   - Use filters and the search function to look for specific values.
   - Export and print the information in the table.

Modifying Active Directory Sites and Networks

You can edit the name of an Active Directory Site and associate networks with the respective site. You can also add additional networks or remove associated networks from the Active Directory Site.

To edit an Active Directory Site:

1. From the Grid tab, select the Microsoft Servers tab -> Active Directory Domains tab and click respective Active Directory Domain name.
2. In the Active Directory Domains Home table, select an Active Directory Site name and click the Edit icon, or click the Action icon next to the respective Active Directory Site name and select Edit from the menu.
3. In the Active Directory Site Properties editor, you can do the following:
   - **Name**: The name of the Active Directory Site. You can edit the name.
   - **Networks**: The networks that are associated with the Active Directory Site. You can click the Add icon to associate new networks with the Active Directory Site.

   To delete an associated network, select the check box adjacent to the network address, and click the Delete icon.

4. You can either click Save and Close or Save to save your settings. Click Cancel to close the editor without saving your settings.

Deleting Active Directory Sites

You can delete Active Directory Sites that are associated with an Active Directory Domain. You cannot delete an Active Directory Site from the Active Directory Domain if the respective Active Directory Site has networks associated with it. You must first delete the associated networks to delete an Active Directory Site.

To delete Active Directory Sites:

1. From the Grid tab, select the Microsoft Servers tab -> Active Directory Domains tab and click the respective Active Directory Domain name.
2. In the Active Directory Domains Home table, select an Active Directory Site and click the Delete icon, or click the Action icon next to the respective Active Directory Site name and select Delete from the menu.
3. The appliance displays a confirmation message. Click Yes to delete the sites or click No to cancel the operation.

Moving Networks Between Active Directory Sites

You can move networks from an Active Directory Site to another using either the Microsoft Servers or the IPAM tab. You can use the Microsoft
Servers tab to move networks only when you select an Active Directory Site.
You can add multiple networks from various Active Directory Sites and move them simultaneously to an Active Directory Site. When the Active Directory Site synchronizes, it always maps to a certain network view. You can only select networks from a network view to which the Active Directory Domain belongs.

To move networks within Active Directory Sites, complete the following:

1. **Microsoft Servers tab**: From the Grid tab, select the Microsoft Servers tab -> Active Directory Domains tab and click respective Active Directory Domain name. In the Active Directory Domains Home table, click the Action icon next to the respective Active Directory Site name and select Move Networks from the menu.
   OR
   **IPAM tab**: From the Data Management tab, select the IPAM tab, select networks that you want to move and click Move Networks from the Toolbar.

2. In the Move Networks wizard, complete the following:
   - **Destination Active Directory Site**: Click Select Site to select the destination Active Directory Site. The appliance displays the Microsoft Sites Selector dialog box listing all the Active Directory sites in the Grid. It also displays the smart folders, if any. You can use the filter and Go to functions to find a specific Active Directory site. To select an Active Directory site, click the site name.
   - **Networks**: You can select networks that you want to move to another Active Directory Site.
     - Go to: Specify an IP address of the network that you want to move to another destination and click Go.
     - Click the Add icon to add networks. To delete a network from the list, select the check box next to the network and click the Delete icon.

3. Click Move to move networks or click Close to exit.

### Moving Multiple Networks to an Active Directory Site

You can move multiple networks to a given Active Directory Site in a single operation. The following rules are applicable:

- Only a super-user can move multiple networks to an Active Directory Site.
- The destination site must belong to an Active Directory Domain that is synchronized in Read/Write mode.
- The appliance assigns the destination Active Directory Site to a network in either of the following cases:
  - If the network is currently assigned to another Active Directory Site within the same Active Directory Domain.
  - If the network is currently not assigned to any Active Directory Site within the Active Directory Domain.
- The Active Directory Sites associated with an Active Directory Domain is different from the destination Active Directory Site.

### Associating Active Directory Sites with Networks

You can associate an Active Directory Site with an IPv4 or IPv6 network or an IPv4 and IPv6 network template. The appliance does not check the synchronization mode of the associated Active Directory Domain when you create or modify a template, but it verifies only when you use the template to create a network.

To assign Active Directory Sites to networks, complete the following:

1. From the Data Management tab, select the DHCP tab -> Networks tab.
2. In the Networks section, select either IPv4 Network or IPv6 Network from the Add drop-down menu and complete the details as mentioned in Adding IPv4 Networks and Adding IPv6 Networks respectively, and complete the following to assign Active Directory Sites to networks:
   - **No Active Directory Site**: Select this if you do not want to associate an Active Directory Site with the network.
   - **Assign these Active Directory Domains/sites**: Select this to assign multiple Active Directory Sites to a network, but note that each Active Directory Site must be associated with a different domain. You cannot add an Active Directory Site, if you have already assigned a domain from the same Active Directory Site. When you select this option, the appliance enables the following:
     - **Active Directory Domain**: The Active Directory Domains that are synchronized from the Microsoft server. Click an Active Directory Domain that you want to associate.
     - To search for a particular Active Directory Domain, specify the respective name and click Go.
     - **Active Directory Sites**: The Active Directory Sites that are associated with the selected Active Directory Domain. Click an Active Directory Site that you want to associate.
     - To search for a particular Active Directory Site, specify the respective name and click Go.
     - **Add >**: Click this to add the selected Active Directory Sites to the network.
     - <Remove>: Click this to remove an Active Directory Site, which you have already added, from the network.
     - <Remove all>: Click this to remove Active Directory Sites, which you have already added, from the list.
   - **Assign the same domains/sites as the selected network**: Click Select Network to assign Active Directory Sites, which are associated with the selected network, to the new network that you are configuring. Select a network from the Network Selector dialog box. The appliance displays the Active Directory Domains and Sites that are associated with the selected network, but you cannot make any changes and the fields are greyed out. Click Clear to clear the entry.

3. You can either click Save and Close to save the settings and close the wizard or click Save and New to save your settings and open a new wizard or click Cancel to close the wizard without saving your settings.
Managing Extensible Attributes and Associated Networks

The appliance creates an extensible attribute for each Active Directory Domain that is synchronized with the Grid. Note the following about extensible attributes:

- The appliance generates a name for the extensible attribute. The appliance displays an error message if you have already created an extensible attribute with the same name.
- Extensible attributes are Read-only and does not support inheritance.
- You can define a single value only and there are no default values.
- The appliance restricts an extensible attribute to IPv4 network and IPv6 network objects.
- You can specify a value for each extensible attribute and it is optional.

Configuring Microsoft Server and LDAP Connections

Active Directory is a distributed directory service that authenticates network users. Active Directory uses LDAP (Lightweight Directory Access Protocol) to access other network services. This protocol is also used when an Active Directory Service entry is configured under Authentication Server Groups. For an Active Directory, the Grid member uses LDAP to communicate with the Microsoft server. Note that the managed Microsoft server must be a part of an Active Directory Domain and it must be a domain controller for the respective domain. The appliance logs an error message in the Microsoft log each time the synchronization happens if the Microsoft server is not a part of the Active Directory Domain or if it is not the domain controller for the respective domain. You can define an LDAP timeout value at the Grid level and override it at the Microsoft server level.

To configure LDAP timeout settings, complete the following:

1. **Grid**: From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar. Select the Microsoft Sync Settings tab in the Grid Properties Editor wizard and click the Advanced tab.
   - **Microsoft Server**: From the Grid tab -> Microsoft Servers tab -> Servers tab, select a Microsoft server and click the Edit icon. In the Microsoft server editor, select the General tab and click the Advanced tab.
2. Complete the following:
   - **LDAP timeout**: Specify the LDAP connection timeout value. The default is 10 seconds. You can specify a value between one and 60 seconds.
     - You can click Override to override the LDAP timeout value at the Microsoft server level. To inherit the settings from the Grid, click Inherit.
3. Save the configuration.

Configuring Server Site Links

You must choose a site link when you create an Active Directory Site on the Microsoft server. The site link describes how the replication occurs between the sites and the protocol, either IP (Internet Protocol) or SMTP (Simple Mail Transfer Protocol), which is used for communication. The appliance uses the default object DEFAULTIPSITELINK when you create an Active Directory Site from the NIOS appliance. If you want to change the site link for a given Active Directory Site, which is already created, you must create the Active Directory Site on the Microsoft server or modify it on the Microsoft server after you create it using the NIOS appliance.

When you create Active Directory sites, the appliance automatically associates them with the default IP site link. The value that you specify for default IP site link must exist on the Microsoft server. Note that the appliance does not display any error message when you create a site with a site link that does not exist on the Microsoft server.

To configure server site links, complete the following:

1. From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar.
   - **Microsoft Server**: From the Grid tab -> Microsoft Servers tab -> Servers tab, select a Microsoft server and click the Edit icon. In the Microsoft server editor, select the General tab and click the Advanced tab.
2. Select the Microsoft Sync Settings tab in the Grid Properties Editor wizard and complete the following in the Advanced tab:
   - **Default IP site link**: Specify the default IP site link in the form of a string. The appliance does not validate it against the Windows server during configuration. The appliance displays an error message during synchronization, if the site link for IP does not match the configured name on the Windows server.
     - You can click Override to override the default IP site link value at the Microsoft server level. To inherit the settings from the Grid, click Inherit.
3. Save the configuration.

Managing Active Directory Sites and Associated Networks

You can manage Active Directory Sites and networks using either the Microsoft servers or the NIOS appliance.

Managing an Active Directory Site from the Microsoft server
You can create, modify, or delete an Active Directory Site from the Microsoft server in both Read-only and Read/Write synchronization modes. When you create an Active Directory Site from the Microsoft server, it is created on the NIOS appliance. This site appears as an Active Directory Site under the corresponding Active Directory Domain and in the respective extensible attribute.

When you make changes on the Microsoft server, the synchronization process ignores any other modifications that you make, but replicates only the name changes to the Grid. When you rename an Active Directory Site, the change reflects:

- in the Active Directory Site and in the respective extensible attribute.
- on all the networks that are associated with the Active Directory Site.

When you delete an Active Directory Site from the Microsoft server, it deletes the Active Directory Site object and removes corresponding extensible attributes. The appliance removes the value from all the network objects that are associated with it.

**Managing an Active Directory Site from NIOS**

You can create, modify, or delete an Active Directory Site from the appliance in Read/Write synchronization mode only. The appliance displays an error message if you perform any of these operations in Read-only mode.

When you rename an Active Directory Site and the associated networks, the changes reflect on the Microsoft server. The appliance displays an error message when you delete an Active Directory Site that is associated with networks. You must first remove the networks that are associated with the site.

You cannot resize or split a network with an associated site in Read-only synchronization mode. You cannot join two networks if any of the involved networks or network containers are associated with a site irrespective of the synchronization mode.

**Managing Network Operations from Microsoft server**

Note that you can perform network operations, such as create, modify or edit networks, in both Read-only and Read/Write synchronization modes. When you create a network, the synchronization process ignores the network if it is not assigned to a Active Directory Site. When the network is attached to the site, the appliance finds a matching network or network container in the configured network view. If it does not exist, the appliance creates a new network or a network container depending on the objects existing in the database. The new network or network container is set as unmanaged and a new extensible attribute is attached to the object to store the site.

Note the following about managing networks:

- When you update a site that is associated with a network, the change is visible on the corresponding network or network container.
- Synchronization process ignores the changes when you update a network. Note that it does not ignore the changes when you modify the Active Directory Site or change an IP address or a CIDR.
- When you delete a network, the appliance removes the extensible attribute that is representing the associated site from the corresponding network or network container.
- If the status is set as managed, it indicates that the network is used for another purpose inside the Grid. The appliance does not remove it from the Grid.
- If the status is set as unmanaged, the appliance deletes the network if there is no other site coming from another Active Directory Domain, which is associated with the network. Otherwise the appliance does not remove the network from the Grid.

**Converting Unmanaged Networks to Managed Status**

When you synchronize a network from the Active Directory server, the network created in NIOS is considered to be unmanaged. You can neither associate a NIOS member or a Microsoft server to manage it nor edit permissions, and other fields. You can only edit extensible attributes and Active Directory sites on the unmanaged network. To perform certain operations on Unmanaged networks, you must first convert them to Managed networks.

The IPAM main page lists all networks that are created during Active Directory synchronization as unmanaged, highlighted in yellow. You can explore unmanaged networks through IPAM's **IP Map** and **IP List** views.

Unmanaged networks can be converted at the IPAM main page and at the device level under **Data Management → Devices**, selecting a device and opening the **Networks** page.

**Managing Network Operations from NIOS**

The appliance denies the operation when you create a network, which is associated with a site, if the respective site belongs to an Active Directory Domain that is synchronized in Read-only mode. Otherwise the appliance creates it on the Microsoft server that is associated with the respective site.

**Restoring Server Data**

When you restore a database backup, the appliance performs the following operations after the standard restore procedure is complete:

- The appliance deletes the cached data that is used for synchronization.
- Synchronization for all configured Microsoft servers starts in Read-only mode. Note that these rules are applicable during upgrade also.
Configuring Identity Mapping

You can enable Identity Mapping on the NIOS appliance to provide Active Directory domain user information if the NIOS appliance is connected to a Microsoft server. This feature supports Active Directory domains whose domain controller is running Windows 2008 server, Windows 2008 R2 server, Windows 2012 server, or Windows 2012 R2 server, or Windows 2016 server. Note that Identity Mapping is not supported for the Windows 2003 server and earlier editions. Note that Identity Mapping is not supported on the TE-810, TE-820, IB-VM-810 and IB-VM-820 appliances.

Each network user being mapped can use different devices to access the Windows environment. So using the identity mapping feature and synchronizing all Microsoft servers on the Infoblox appliance provide visibility of user interaction with their environments. By enabling this feature, you can monitor Active Directory domain users, the IP addresses they log on to, the login status, and the time duration of their current status in the IPAM tab.

To view user information, you must first enable this feature at the Grid level. You can enable this feature even when you have not installed an MS Management license on the appliance. However, you cannot configure DNS, DHCP, and Active Directory sites synchronization unless you install an MS Management license on the appliance.

When you enable this feature, the appliance remotely communicates with all synchronized Microsoft servers (Domain Controllers, an Exchange server, or a domain member) to pull event logs. The identity mapping information displayed is as accurate as these event logs are available in the Microsoft authentication logs. Therefore, it is necessary to assign Grid members to Microsoft servers to collect user information from Windows event logs. For information, see Assigning Grid Members to Microsoft Servers.

Note: The identity mapping information displayed on NIOS completely depends on live event logs that are available on the Microsoft servers. The appliance pulls event logs incrementally. So subsequent requests pull only the latest logs since the last successful synchronization. To avoid data loss, depending on the expected activities, you must consider the size of the event log file on the Microsoft server and how often you want to synchronize the data with the appliance before the event log file rolls over.

Prerequisites on the Microsoft Server


The identity mapping information is collected successfully only when the Microsoft users belonging to a Domain User group and Event Log Reader group start a RPC session and access MS-EVEN6. The synchronization process is successful when they have this permission. The synchronization process fails unless appropriate permissions are granted. The failed operations are logged in the Microsoft logs. The NIOS appliance tries to collect user information again in the next synchronization.

Administrative Permissions

Only superusers can view identity mapping information. Limited-access admin groups can view identity mapping information only if they have network permissions. For example, if the users have permissions to only DNS zones, they may not be able to view identity mapping information because they do not have network permissions. The appliance does not display a warning message if admins do not have correct permissions. For information about network permissions, see Administrative Permissions for IPv4 and IPv6 Networks and Shared Networks.

About User Sessions

A user session is an abstract concept to specify a single user logging with a network address for a finite period of time. A user session starts when a Kerberos account authentication event or login event is received and ends when a logout is received, although such an event may never be received. In such cases, a session is considered to be timed out. Network user associations are unique for a finite period of time. A single login involves a number of login and logout events. In order to consolidate and improve system performance, Infoblox uses the concept of consolidation window. If a login event or Kerberos service ticket is received within the consolidation window, then that session is considered as an extension from the previous session. If a login event is received outside this window, it is considered as a new session. The number of network users you see depends on the length of the consolidation window.

For example, consider the following sample events occurred on the Microsoft server when the consolidation window is set to 10 minutes:

Kerberos Authentication Request: 10:00:00
Kerberos Service Ticket Request: 10:00:01
Account Logon: 10:00:02
Account Logoff: 10:00:03
Account Logon: 10:00:05
Account Logoff: 10:00:07
Account Logon: 10:00:10
Account Logoff: 10:00:11
The sample user session for the above events:

<table>
<thead>
<tr>
<th>User Name</th>
<th>IP Address</th>
<th>First Seen Time (UTC)</th>
<th>Last Seen Time (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>John</td>
<td>10.10.10.10</td>
<td>10:00:00 AM (UTC)</td>
<td>10:00:11 AM (UTC)</td>
</tr>
</tbody>
</table>

If another login request is received at 10:30 AM (10 minutes after the last seen event), then it is considered as a different session:

<table>
<thead>
<tr>
<th>User Name</th>
<th>IP Address</th>
<th>First Seen Time (UTC)</th>
<th>Last Seen Time (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>John</td>
<td>10.10.10.10</td>
<td>10:00:00 AM (UTC)</td>
<td>10:00:11 AM (UTC)</td>
</tr>
<tr>
<td>John</td>
<td>10.10.10.10</td>
<td>10:30:00 AM (UTC)</td>
<td></td>
</tr>
</tbody>
</table>

If a Kerberos service ticket is received instead of a login event, then the previous session is extended and is updated as Last Seen Time in the first user session:

<table>
<thead>
<tr>
<th>User Name</th>
<th>IP Address</th>
<th>First Seen Time (UTC)</th>
<th>Last Seen Time (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>John</td>
<td>10.10.10.10</td>
<td>10:00:00 AM (UTC)</td>
<td>10:30:00 AM (UTC)</td>
</tr>
</tbody>
</table>

The appliance displays separate entries (counts) for the following scenarios:

- Multiple users logging in from the same IP address. For example, User 1 logged in with 10.10.10.10 address counts as one network user and User 2 logged in with 10.10.10.10 address counts as another network user.
- Same user logging in from multiple IP addresses. For example, a single user can log in to multiple workstations, each with a different IP address.
- Same user logging from the same IP address at a different time intervals.

**Network User Count Displayed for Different Login Scenarios**

If you are configuring multiple Domain Controllers belonging to different organizations, then you must configure them in different network views. For example, if the same user logs in to multiple Domain Controllers with the same IP, it creates multiple entries for each login. In this case, there is a chance of overwriting an entry by subsequent events. If Domain Controllers are configured in different views, then separate entries are displayed for different network views. You can configure multiple Domain Controllers within the same network view if they serve the same organization, possibly using a load balancing method.

**Note:** The appliance displays user information only for the managed networks.

The following table illustrates how the appliance displays counts for different login scenarios:

**Table 34.1 Network User Count Displayed for Different Login Scenarios**

<table>
<thead>
<tr>
<th>Login Scenarios</th>
<th>Appliance Displaying User Mapping Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile user logging in to the Microsoft Exchange server</td>
<td>Note that you must first synchronize both the Domain Controller and Microsoft Exchange server with the appliance to get user mapping information for this scenario. For this example, two entries are displayed. 1. User name and IP address of the Microsoft Exchange server on the Domain Controller. 2. User name and IP address of the mobile device on the Microsoft Exchange server.</td>
</tr>
<tr>
<td>Multiple users from the same IP address</td>
<td>Appliance displays separate entry (user name and IP address) for each user.</td>
</tr>
<tr>
<td>Same user from multiple IP address</td>
<td>Appliance displays separate entry (user name and IP address) for each user.</td>
</tr>
</tbody>
</table>

**Login and Logout Timestamps**

Note that all timestamps are displayed in the time zone of the admin account that you use to log in to the appliance. There is a possibility of missing the login and logout events as described in the following cases:

- There is a chance of missing a login event when NIOS retrieves event logs from the Microsoft server after a user logs in and the event log has already rolled over.
- There is a possibility of missing a logout or session end notifications when the user shuts down the workstation or leaves the system. In such cases, the Microsoft event log does not specifically indicate a logout. The logout events that are missed on the Domain Controller or Exchange server are missed on NIOS as well.
To maintain accuracy, the login timestamp is estimated as logout timestamp minus (-) the idle timeout. However, when a login or Kerberos Authentication event is received, the login timestamp is updated to the value available in the Kerberos authentication event or the login event. To maintain accuracy of the logout time data, the appliance allows you to configure the length of idle time in the Grid Properties Editor wizard. After this time interval, the status of the user changes to **Timed Out**. For information about how to set timeout length, see [Configuring Active User Timeout Session](#).

**Note:** The **Timed Out** and **Logged Out** user information is periodically removed from the database.

### Viewing Active Directory User Information

To view Active Directory user information, you must first enable identity mapping feature at the Grid level. For information about enabling Identity Mapping feature, see [Enabling Identity Mapping](#). After you enable the identity mapping feature, you must synchronize the appliance with all Microsoft servers in order for the appliance to gather user and device mapping information from the Microsoft servers. You can view Active Directory user information in the **Network Users** tab. For more information, see [Viewing Active Network Users](#).

To synchronize the appliance with Microsoft servers:

1. From the **Grid** tab, select the **Grid Manager** tab, and then select **Grid Properties** -> **Edit** from the Toolbar.
2. Select the **Microsoft Integration** tab in the **Grid Properties Editor** wizard, and complete the following:
   - Synchronize Network Users with all MS servers: Select this check box to synchronize users with all Microsoft servers that are managed by the Grid in order for the appliance to gather user and device mapping information from the Microsoft server authentication logs. You can override this value at the Microsoft server level.

**Note:** On an Infoblox appliance, the **Enable Network Users Feature** and **Synchronize Network Users with all MS servers** options are disabled by default for all new installations.

3. Save the configuration.

### Monitoring Managed Microsoft Servers

You can monitor the status of managed Microsoft servers from the Dashboard and from various panels in the **Grid** tab. Grid Manager also maintains a log for each managed Microsoft server. You can monitor Microsoft servers and their services as follows:

- You can view the **Microsoft Servers Status** widget on the Dashboard. For information, see [Microsoft Servers Status Widget](#).
- You can view the status of Microsoft servers. For information, see [Viewing DNS and DHCP Service Status on Microsoft Servers](#).
- You can view the logs of the Microsoft servers. For information, see [Viewing Synchronization Logs](#).

### Viewing DNS and DHCP Service Status on Microsoft Servers

Each Microsoft server reports the following statuses:

- **Service status (DNS and DHCP):** Displays the status of the service on the actual Microsoft server, based on the latest polling of the service by the managing member. The monitor and control setting has an effect only on the service status, and therefore can affect the overall status.
- **Overall status:** Displays the service status for each service that is enabled for synchronization with the Microsoft server. The overall status ignores any service status for which the monitor and control setting is disabled.
- **Synchronization status:** Displays the synchronization status for each service that is enabled for synchronization on the respective Microsoft server. The synchronization status is not affected by the monitor and control setting. For more information, see [Viewing DNS and DHCP Service Status on Microsoft Servers](#).

**Note:** When you disable monitor and control settings, Grid Manager displays **unknown** using gray color for such services. When you enable monitor and control setting of a given service, Grid Manager displays the last known status that is obtained before the setting was first disabled. The appliance later updates to the latest status as soon as the monitoring resumes and Grid Manager displays the new status.

You can view details about the managed Microsoft servers by navigating to the **Grid** tab -> **Microsoft Servers** tab -> **Servers** tab. For each Microsoft server, the panel displays the following by default:

- **Name:** The FQDN of the Microsoft server.
- **Status:** The connection status, which can be one of the following:
  - **Running:** The Grid member is connected to the Microsoft server.
  - **Connecting:** The Grid member is connecting to the Microsoft server.
  - **Error:** The Grid member failed to connect to the Microsoft server. Check the Microsoft log for any messages to determine the reason for the failure.
  - **Unknown:** The Microsoft server is disabled. The Grid member does not try to connect to disabled servers.
- **IP Address:** The IP address of the Microsoft server.
**DNS:** The status of the DNS service on the Microsoft server. When you disable DNS synchronization, NIOS does not display any status icon. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td></td>
<td>The DNS service is functioning properly.</td>
</tr>
<tr>
<td>Red</td>
<td></td>
<td>The Microsoft server is unavailable.</td>
</tr>
<tr>
<td>Yellow</td>
<td></td>
<td>The DNS service is starting or stopping.</td>
</tr>
<tr>
<td>Gray</td>
<td></td>
<td>The DNS service is stopped or management of the Microsoft DNS server is disabled.</td>
</tr>
</tbody>
</table>

**DHCP:** The status of the DHCP service on the Microsoft server. When you disable DHCP synchronization, NIOS does not display any status icon. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td></td>
<td>The DHCP service is functioning properly.</td>
</tr>
<tr>
<td>Red</td>
<td></td>
<td>The Microsoft server is unavailable.</td>
</tr>
<tr>
<td>Yellow</td>
<td></td>
<td>The DHCP service is starting or stopping.</td>
</tr>
<tr>
<td>Gray</td>
<td></td>
<td>The DHCP service is stopped or management of the Microsoft DHCP server is disabled.</td>
</tr>
</tbody>
</table>

- **Comment:** Displays any comments that were entered for the Microsoft server.
- **Site:** Displays any values that were entered for this pre-defined attribute. You can add the following columns for display:
- **Version:** The Windows version of the managed server.
- **Managing Member:** The hostname of the Grid member that manages the server.
- **Synchronization Status:** Displays the synchronization status as follows:
  - **Running:** The Microsoft server is synchronizing data with the Grid member.
  - **Connecting:** The Grid member is trying to connect to the server.
  - **Error:** Synchronization failed between the member and server. You can check the messages in the Microsoft server log to determine the reason for the failure.
- **Last Changed:** Displays information about when the status was last updated for Microsoft DNS and DHCP services. It corresponds to the last time information was exchanged with the server.
- **AD Domain:** Displays the AD domain of the Windows server. This is displayed only if the Windows server belongs to an Active Directory domain.
- **Root AD Domain:** Displays the root AD domain of the Windows server. This is displayed only if the Windows server belongs to an Active Directory domain.

You can also do the following:

- Add Microsoft servers. Click the Add icon.
- Edit the properties of a Microsoft server.
  - Click the check box beside a server and click the Edit icon, or click the Action icon next to the respective Microsoft server and select **Edit** from the menu. For information, see [Setting Microsoft Server Properties](#).
- Delete a Microsoft server.
  - Click the check box beside a server and click the Delete icon, or click the Action icon next to the respective Microsoft server and select **Delete** from the menu. For information, see [Removing a Managed Microsoft Server](#).
- Manage DNS and DHCP services of a Microsoft server.
  - Click the check box beside a server and click the Manage Server Services icon, or click the Action icon next to the respective Microsoft server and select **Manage Server Services** from the menu to view the service status. You can mouse over the DNS and DHCP service icons and click the Start/Stop service icon to start or stop a service, or click the Edit Service icon to edit the service properties. For information about setting DHCP server properties, see [Setting Microsoft DHCP Server Properties](#). For information about setting DNS server properties, see [Specifying Forwarders for Microsoft Servers](#).
- View detailed server status information, as described in [Viewing Detailed Status Information](#).
- Click **Test MS Server** to test the Microsoft server connection. The appliance validates the Microsoft server and displays the test code and the test result data for services that you have enabled. To test the Microsoft server, click the check box beside a server and click the Test Microsoft Server icon, or click the Action icon.
next to the respective Microsoft server and select **Test Microsoft Server** from the menu. For more information, see **Assigning Grid Members to Microsoft Servers**.

- View extensible attributes associated with the Microsoft server.
  - Click the Action icon

next to the respective Microsoft server and select **Extensible Attributes** from the menu. For information, see **Assigning Grid Members to Microsoft Servers**.

- Define permissions for Microsoft servers.
  - Click the Action icon

next to the respective Microsoft server and select **Permissions** from the menu.

- Use filters and the **Go To** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see **Using Quick Filters**.
- Sort the displayed data in ascending or descending order by column.
- Export the list of Microsoft servers to a .csv file.
  - Click the Export icon.
  - Print the list of Microsoft servers.
  - Click the Print icon.

**Viewing Detailed Status Information**

You can view more status information by selecting a server from the Microsoft servers panel and clicking the Action icon

next to the respective Microsoft server and selecting **Detailed Status** from the menu or clicking the Detailed Status icon. The **Detailed Status** panel displays the following information:

- **Synchronization Status**: The status icon indicates the synchronization status as follows:
  - Green: The Microsoft server is synchronizing data with the Grid member.
  - Red: Synchronization failed between the member and server. You can check the messages in the Microsoft server log to determine the reason for the failure.
- **DNS Service Status**: For information about the status icons, see **Viewing DNS and DHCP Service Status on Microsoft Servers**.
- **DNS Service Status Last Updated**: The date and time of the last DNS service status update from the Microsoft DNS server.
- **DHCP Service Status**: For information about the status icons, see **Viewing DNS and DHCP Service Status on Microsoft Servers**.
- **DHCP Service Status Last Updated**: The date and time of the last DHCP service status update from the Microsoft DHCP server.
- **Active Directory Sync Status**: The Active Directory Site is synchronizing data with the Grid member when the status icon is green.
- **Active Directory sync status last updated**: The date and time of the last Active Directory Site update from the Microsoft server.

Note the following guidelines about status information:

- Grid Manager does not display any status information if there is no synchronization between DHCP and DNS.
- If the appliance has not received any information when the services are enabled, then the Synchronization Status icon is displayed in red, whereas the DNS and DHCP status icons are displayed in grey.

**Viewing Synchronization Logs**

Grid Manager maintains a synchronization log file for each Microsoft server managed by a Grid member. It logs events related to the synchronization process, depending on the logging level that you configured in the **Logging** tab of the **Microsoft Server Properties** editor described in **Setting Microsoft Server Properties**.

The log files are rotated and compressed once they reach 40MB. To view the log file of managed Microsoft server:

1. From the **Administration** tab, select the **Logs** tab -> **Microsoft Logs** tab.
2. If there is more than one managed server in the Grid, you can select the Microsoft server whose logs you want to view.
3. The log file contains information related to the synchronization of the Microsoft DNS and DHCP data, as follows:

- **Timestamp**: The date and time of the log message. The time zone is the time zone configured in the User Profile.
- **Source**: Identifies the event that generated the message, such as a server synchronization or zone synchronization.
- **Level**: Indicates the severity of the message, which can be one of the following:
  - **Debug**: Provides information about all events associated with synchronization.
  - **Information**: The Grid member is synchronizing with the Microsoft server and these messages provide normal status information.
  - **Warning**: The Grid member synchronized the data, but there was an issue, which is detailed in the Message section.
  - **Error**: The Grid member encountered an error during the synchronization, it skips the object with the error, logs the error in the
Microsoft log, and continues to synchronize the rest of the data. The Grid member logs the error at each synchronization until you resolve the issue and it can synchronize the object successfully.

- **Error**: The Grid member failed to synchronize an object, such as a DNS zone or DHCP scope, due to the error described in the Message section.

- **Object Type**: The type of object that corresponds to the entry, such as FQDN or ADDRESS.
- **Object Name**: The name of the object that corresponds to the entry.
- **Message**: Detailed information about the event.

You can also do the following in the log viewer:

- Toggle between the single line view and the multi-line view.
- Navigate to the next or last page of the file using the paging buttons.
- Refresh the view.
- Click the Follow icon to have the appliance automatically refresh the log every five seconds.
- Download the log.
- Clear the contents of the log.
- Sort the data in ascending or descending order by column.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Export or print the content of the log.

### Chapter 35 Managing Microsoft DNS Services

This chapter provides guidelines for using Grid Manager to manage Microsoft DNS servers and for synchronizing DNS data between Microsoft servers and the Grid. It discusses some features of the Microsoft DNS servers only as they relate to the synchronization of data. Please review the Microsoft documentation for complete information about Microsoft DNS servers and their features.

In addition, if you encounter technical issues with your Microsoft DNS servers, contact Microsoft Technical Support or consult the Microsoft Support site at [http://support.microsoft.com/](http://support.microsoft.com/). Some Windows versions require certain updates and hotfixes installed, so the Microsoft server can synchronize with the Grid member. For information about these requirements, see Requirements.

The topics in this chapter include:

- Managing Microsoft DNS Servers
  - Synchronizing DNS Data
  - Enabling and Disabling DNS Zone Synchronization
  - IDN Support for Synchronized DNS Data
  - Synchronizing with Multiple Servers
- Managing Synchronized DNS Data
  - Adding Zones to Microsoft Servers
  - Setting Zone Properties
  - Deleting and Restoring Synchronized Zones
  - Managing Resource Records in Synchronized Zones
- Synchronizing Updates
  - Synchronizing Delegations
  - Synchronizing AD-Integrated Zones
  - Resolving Conflicts
- Viewing Members and Managed Servers
- Specifying Forwarders for Microsoft Servers
- Disabling and Removing Microsoft DNS Servers

### Managing Microsoft DNS Servers

After you configure a Grid member to manage a Microsoft DNS server, the Grid member connects to the Microsoft server and starts synchronizing DNS data from the Microsoft server to its database. First, it synchronizes the Microsoft server properties and its list of zones. Then it synchronizes each zone individually, including its properties and resource records.

The synchronization time varies, depending on different factors, such as the number of managed Microsoft servers and the amount of data being synchronized. The synchronized data is then replicated to the Grid Master through the Grid replication process.

If the server is managed in read/write mode, admins can update the synchronized DNS data, control the DNS service of the server, and specify forwarders for it as well.

### Synchronizing DNS Data

Managing members synchronize the properties and resource records for the following types of DNS zones:

- Authoritative forward-mapping zones
- IPv4 and IPv6 reverse-mapping zones
- Stub zones
- Delegations
- Active Directory-integrated zones
Grid members synchronize most of the resource records supported by Microsoft servers, except for WINS, WINSR, and ATMA records. They synchronize all the resource records supported by Infoblox DNS servers, as well as unsupported records, such as ISDN and X25 records. You can view the unsupported records in Grid Manager and delete them, but you cannot edit them. Note that Grid Manager and Microsoft DNS servers display some resource records, such as SIG records, in a different format. You can enable and disable zone synchronization for individual Microsoft DNS zones. For information, see Enabling and Disabling DNS Zone Synchronization.

Grid members do not synchronize the following DNS zones supported by Microsoft servers:

<table>
<thead>
<tr>
<th>Infoblox Terminology</th>
<th>Microsoft Terminology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding zones</td>
<td>Conditional forwarders</td>
</tr>
<tr>
<td>Cached zones</td>
<td>Stub zones</td>
</tr>
<tr>
<td>Root zone</td>
<td>Root zone (Dot zone)</td>
</tr>
<tr>
<td>0.in-addr.arpa</td>
<td>0.in-addr.arpa (0.0.0.0)</td>
</tr>
<tr>
<td>127.in-addr.arpa</td>
<td>127.in-addr.arpa (127.0.0.1 - loopback)</td>
</tr>
<tr>
<td>255.in-addr.arpa</td>
<td>255.in-addr.arpa (255.255.255.255 - broadcast)</td>
</tr>
<tr>
<td>TrustAnchors</td>
<td>Trust Anchors</td>
</tr>
</tbody>
</table>

You cannot use Grid Manager to create the unsupported zones and assign them to a Microsoft server. Any zone on the Grid that has the same name as a forwarding, cached or root zone on the Microsoft server is not synchronized. In addition, Grid members do not synchronize the contents of a zone if the Microsoft server is a secondary server.

Subdomains defined within a Microsoft DNS zone are not synchronized unless they contain at least one resource record. For example, in the corpxyz.com zone, any resource record defined in a subdomain of the corpxyz.com zone is synchronized. If the subdomain sub.corpxyz.com zone has no resource record, it is not synchronized.

The following zones and resource records are supported on Microsoft servers running Windows Server 2008 only. Therefore, Grid members can only synchronize these DNS zones and resource records with Microsoft servers running Windows Server 2008.

- IPv6 reverse-mapping zones
- Global Names zones
- DNAME records
- NAPTR records
- DNSSEC records

Enabling and Disabling DNS Zone Synchronization

You can enable or disable zone synchronization for multiple zones:

1. From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and then click the Edit icon.
2. In the Authoritative Zone editor, click Name Servers.
3. Select Use this set of name servers, and enter the details as specified in Assigning Zone Authority to Name Servers.
4. Save the configuration.

Enabling and Disabling DNS Zone Synchronization for Multiple Zones

You can enable or disable Microsoft zone synchronization for multiple zones:

1. From the Data Management tab, select the DNS tab -> Zones tab, and select the zone check boxes. You can either select a single zone or multiple zones.
2. Expand the Toolbar and click the arrow beside MS Zone Synchronize to select an option.
   - Enable: Click Enable to enable zone synchronization for the selected zones. Click Yes in the Enable MS Zone Synchronization dialog box to enable synchronization or click No to cancel the process.
   - Disable: Click Disable to disable zone synchronization for the selected zones. Click Yes in the Disable MS Zone Synchronization dialog box to disable synchronization or click No to cancel the process.
Considerations about Zone Synchronization

Before you enable and disable zone synchronization for a Microsoft DNS zone, consider the following:

- Zone synchronization is enabled by default.
- A zone must be synchronized at least once before you can disable synchronization.
- Zones defined on a Microsoft DNS server are listed in the NIOS appliance, regardless of whether they are synchronized or not.
- When you delete a zone on the Microsoft server, it is automatically deleted from NIOS, irrespective of its synchronization setting.
- When you create a zone on the NIOS appliance and disable zone synchronization, the zone is not created on the Microsoft server until you enable zone synchronization.
- When you disable zone synchronization, you can perform operations for which you have access rights on the NIOS appliance. This includes changes made directly to the zone or as a result of changes made in another zone. Examples: delegation creations and editing name servers.
- When you disable synchronization for a zone and perform certain operations on the respective zone, the outcomes of those operations are not replicated on any Microsoft servers assigned to the zone. For Microsoft primary servers, any resource records or zone properties (including name servers) that you create, modify, or delete on the NIOS appliance are not copied to the Microsoft server. For Microsoft secondary servers and stub servers, any zone properties (including name servers and masters) that you create, modify, or delete on the NIOS appliance are not copied to the Microsoft server.
- When you disable synchronization for a zone, the zone retains the Microsoft server that was last selected as the master before synchronization was disabled. The master retains its role when you enable synchronization again.
- When you disable synchronization, NIOS completes the ongoing process. The synchronization effectively stops at the end of the synchronization. NIOS resumes the synchronization of the zone as soon as the member assigned to the master MS server is notified through Grid replication that the zone is no longer disabled for synchronization and the zone is overdue for synchronization. This is based on the last time the zone was successfully synchronized and the synchronization interval at the time of re-enabling the synchronization.
- NIOS retains the zone synchronization disable setting when you enable or disable the DNS synchronization setting of any MS server that is assigned to the zone.

IDN Support for Synchronized DNS Data

Infoblox Grid supports IDNs for synchronized DNS data between the appliance and Microsoft servers. For more information about IDNs, see [Supp ort for Internationalized Domain Names](#).

The appliance stores IDNs in punycode and Microsoft server stores IDNs in \xyz format. Due to this difference at the DNS protocol level, IDNs are not allowed in a zone name when you configure NIOS (primary or secondary) and Microsoft (primary or secondary) servers. For information, see [IDN Support Limitations for Synchronized Data](#). If synchronized data between NIOS and Microsoft servers contain IDNs, the IDNs are preserved on the primary server. When a Microsoft server is the secondary server for a zone, MMC (Microsoft Management Console) displays the zone content that contains IDNs in punycode only. Make sure that you use a zone name that complies with the DNS protocol when manually configuring an authoritative zone.

A Microsoft server serves a resource record that contains an IDN in \xyz format when it is configured as the primary server and NIOS as the secondary server. For example, use the \xyz\xyz\xyz.com representation on NIOS for .com, a zone added on the Microsoft server.

You can add resource records that contain IDNs for the following configurations:

- NIOS is the primary server and Microsoft server is the secondary server: You can add records in IDNs or punycode. The appliance preserves IDNs and does not encode punycode to IDNs. Note that you cannot add a resource record that contains an IDN on the Microsoft server when it is configured as the secondary server.
- Microsoft server is the primary server and NIOS is the secondary server: You can add records on both NIOS and Microsoft servers. You can use IDNs or punycode. You can add IDN records on both servers in this scenario.

The following table summarizes how the servers display resource records that contain IDNs after synchronization:

<table>
<thead>
<tr>
<th>Primary Server</th>
<th>Input</th>
<th>Secondary Server</th>
<th>Input</th>
<th>NIOS displays record s in...</th>
<th>Microsoft server disp lays records in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIOS</td>
<td>Punycode</td>
<td>Microsoft</td>
<td>NA</td>
<td>Punycode</td>
<td>Punycode</td>
</tr>
<tr>
<td>NIOS</td>
<td>IDN</td>
<td>Microsoft</td>
<td>NA</td>
<td>IDN</td>
<td>Punycode</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Punycode</td>
<td>NIOS</td>
<td>Punycode</td>
<td>Punycode</td>
<td>Punycode</td>
</tr>
<tr>
<td>Microsoft</td>
<td>IDN</td>
<td>NIOS</td>
<td>IDN</td>
<td>IDN</td>
<td>IDN</td>
</tr>
</tbody>
</table>

IDN Support Limitations for Synchronized Data

You cannot configure an authoritative zone and stub zone that contains IDNs for the following configurations:

- When NIOS is the primary server and Microsoft server is the secondary server.
- When Microsoft server is the primary server and NIOS is the secondary server.

Synchronizing with Multiple Servers

Copyright ©2019, Infoblox, Inc. All right reserved.
Because a Grid member can manage multiple Microsoft servers, it could potentially manage multiple servers assigned to the same zone. For example, a Grid member could manage a Microsoft server that is the primary server of a zone and one or more Microsoft servers that are secondary servers of the same zone. It could also manage multiple Microsoft servers that are secondary servers for the same zone.

If a Grid member manages the primary server and at least one secondary server of a zone, the Grid member always synchronizes DNS data with the primary server only. It never synchronizes data with the secondary server, even if the primary server fails. If a Grid member manages several Microsoft servers that are secondary servers of the same zone, it synchronizes DNS data as follows:

- If each Microsoft server is assigned to a different DNS view, the Grid member synchronizes data with each one.
- If the Microsoft servers are synchronized to the same DNS view, the Grid member selects a principal server for synchronization purposes, as follows:
  - The first Microsoft server that is assigned as the DNS secondary server is designated principal server.
  - If the secondary servers are managed in read-only and read/write modes, the Grid member always selects a server that is managed in read/write mode.
  - If a Microsoft server fails three successive synchronizations, it loses its principal server status. The Grid Master checks the date that each server last became a principal server and selects the server that has not been the designated principal server the longest.

Note that a Grid member could fail to synchronize with a Microsoft server due to errors, such as a disabled account or an expired password. In these situations, the failure count is reset and is not increased. This prevents the Microsoft server from losing its master status to another Microsoft server that could experience the same errors.

When a zone is served by multiple Microsoft servers, the **MS Sync Server** column of the **Zones** tab shows which Microsoft server is actually performing the synchronization of that zone with the Grid.

**Managing Synchronized DNS Data**

When Grid members are configured to manage Microsoft servers in read/write mode, you can use Grid Manager to view, edit and delete the DNS data of those servers. You can add new zones and assign them to a Microsoft server. You can modify the properties of zones synchronized from the Microsoft server and edit their resource records as well. All updates are synchronized to the Microsoft servers at regular intervals. The following sections provide guidelines for managing the zones and resource records served by Microsoft servers:

- Adding Zones to Microsoft Servers
- 5800380
- 5800380
- 5800380

Synchronized zones also support the following features:

- You can import data to zones synchronized with Microsoft servers. Note that the import fails if you try to import unsupported records to a Microsoft zone. For information about importing records, see Importing Zone Data.
- You can copy records to and from zones synchronized with Microsoft servers. When copying records to a Microsoft zone, you can copy only those records that are supported by Microsoft servers. For information about copying records, see Defining a Match Destinations List.

**Adding Zones to Microsoft Servers**

From Grid Manager, you can create zones and assign Microsoft servers as their primary or secondary servers. The managing Grid member then synchronize these zones to the appropriate Microsoft servers.

From Grid Manager, you can add the following types of zones to Microsoft servers:

- Authoritative forward- and reverse-mapping zones — For information, see Configuring Authoritative Zones.
- Forward- and reverse-mapping stub zones — For information, see Configuring Stub Zones.
- Delegations — For information, see Configuring a Delegation.

Note that you cannot add a zone on a Microsoft server and configure it to be served by an Infoblox Grid member. For example, on the Microsoft server, you cannot add a zone and assign a Grid member as its primary server and the Microsoft server as the secondary server. You must add such a zone from Grid Manager.

Following are guidelines for adding zones to a Microsoft server:

- The primary or secondary server of the zone must be a Microsoft server.
- If the primary server is a domain controller, you can enable the option to store the zone in Active Directory, making it an AD-integrated zone. Note that you can enable Active Directory integration only after the Microsoft server has been synchronized at least once because its AD ability is not known before the synchronization.
- You do not have to assign a Grid member as the primary or a secondary server of the zone. For example, a zone can have a Microsoft server as its primary server and an external secondary server.
- The zone must be in the same DNS view to which the DNS data of the Microsoft server was synchronized. You cannot add a zone served by the Microsoft server to a different DNS view.
- The zone does not inherit the properties from the Grid or from the DNS view. It uses the Infoblox-defined defaults. You can change the property values, as described in 5800380.
- You can set certain zone properties that are not supported and synchronized to the Microsoft server. For example, you can define extensible attributes and administrative permissions. When you set these properties, they apply to the zones only when they are managed from Grid Manager.
- Infoblox does not support all the zone properties of a Microsoft DNS server. When a Grid member synchronizes zones that were created...
on Grid Manager to the Microsoft server, the zones contain default values for all unsupported properties.

- If you set the Disable option, the zone status is set to “Paused” on the Microsoft server. A zone in a “Paused” status is not served to DNS clients, nor is it available for zone updates.
- Setting the Disable option does not stop synchronization. Grid members synchronize disabled zones.
- The member learns the Windows version of the Microsoft server after its first successful synchronization. Certain zones and resource records are dependent on a specific Windows version. You cannot assign these zones to Microsoft servers whose versions are unknown or insufficient.
- If the member is a secondary server for a zone with a Microsoft primary server, the member obtains the zone data through DNS zone transfers from the Microsoft primary server, not through synchronizations. This ensures that the zone data is always current on the Infoblox secondary server, as it does not have to wait for synchronizations to update its data.

### Setting Zone Properties

When the primary server of a zone is a Microsoft server, it does not inherit its properties from the Grid. Zones that are synchronized from a Microsoft server retain their original properties. Zones that Grid Manager admins create assume the Infoblox-defined default values. To modify the properties of a synchronized zone:

1. From the Data Management tab, select the DNS tab -> Zones tab -> DNS_view -> zone check box and click the Edit icon.
2. In the Authoritative Zone editor, you can do the following in each tab:
   - **General:** You can add or edit comments, and set the Disable and Lock options. Setting the Disable option sets the status of the zone to “Paused” on the Microsoft server. Grid members synchronize disabled zones to Microsoft servers.
   - **Name Servers:** You can modify the name servers assigned to the zone. For information, see Assigning Zone Authority to Name Servers.
   - **Settings:** If the zone was synchronized from a Microsoft server, this tab displays the original settings from the Microsoft server. If the zone was created using Grid Manager, then it inherits the TTL values from the Grid. Note that these values might be different from those on the Microsoft server. To change any of these values, see Configuring DNS Service Properties.
   - **Zone Transfers:** In this tab, you specify the servers to which zone transfers are allowed. For information about zone transfers, see Enabling Zone Transfers. Set the following parameters, depending on whether the primary or secondary servers of the zone are Infoblox or Microsoft DNS servers:
     - If the primary server is an Infoblox, Microsoft or external primary and the secondary servers are both Infoblox and Microsoft DNS servers, this tab displays two separate tables where you can specify zone transfer settings for the Infoblox DNS servers and the Microsoft DNS servers.
     - **Zone Transfer Settings for Infoblox Members:** Specify the settings as described in Configuring Zone Transfers.
     - **Zone Transfer Settings for Microsoft Servers:** Note that you cannot use a named ACL for access control though you can use individual ACEs. For information about named ACLs and access control, see Configuring Access Control. You can set access control for zone transfers for Microsoft servers to one of the following:
       - **None:** Does not allow zone transfers to any name server.
       - **Any:** Allows zone transfers to any IP address.
       - **Any Name Server:** Allows zone transfers to any name server in the Name Servers table.
       - **Address:** Allows zone transfers to the IP address that you specify.
     - If both the primary and secondary servers are Microsoft servers, the dialog box displays the Zone Transfer Settings for Microsoft Servers table only.
     - If no Microsoft servers are primary or secondary servers, then the dialog box displays the Zone Transfer Settings for Infoblox Members table only.
   - **Updates:** In this tab, you specify whether the zone can accept dynamic DNS updates. For information about dynamic DNS updates, see Chapter 21, Configuring DDNS Updates. If the primary server is a Microsoft server, regardless of the secondary servers, the Updates tab displays the following:
     - **Dynamic Updates:** Select one of the following:
       - **None:** The zone does not accept dynamic updates.
       - **Secure Only:** This appears only if the zone is AD-integrated. The zone accepts GSS-TSIG-signed updates only.
       - **Nonsecure and Secure:** The zone accepts both nonsecure and GSS-TSIG-signed updates.
   - **Active Directory:**
     - **Automatically create underscore zones:** This option allows the appliance to create the following subzones that the DNS server must have to answer AD-related DNS queries:
       - _msdcs.zone
       - _sites.zone
       - _tcp.zone
       - _udp.zone
       - domainDNSzones.zone
       - forestDNSzones.zone
     - Note that these zones are automatically generated. You cannot edit these zones or import data into them. They cannot be modified, thus providing protection against forged updates.
   - **Extensible Attributes:** Extensible attributes apply to the zones only when they are managed from Grid Manager. For information, see Using Extensible Attributes.
   - **Permissions:** These permissions apply to Infoblox Grid Manager administrators only. For information, see About Administrative Permissions.
Deleting and Restoring Synchronized Zones

When you delete a synchronized zone from the Grid, Grid Manager moves the zone and its resource records to the Recycle Bin. It deletes the zone and its resource records from the Microsoft server at the next synchronization. Note that if you delete a zone on Grid Manager and plan to add it back to the database with different properties or resource records, ensure that you wait until after the deletion is synchronized to the Microsoft server to add the new zone. Otherwise, if you delete a zone and add a new zone with the same name within a synchronization interval, Grid Manager will synchronize the zone properties and resource records from the Microsoft server to the newly added zone on Grid Manager.

If a zone has subzones, you can choose to remove them and their resource records or "reparent" them to the parent zone of the one you are removing. For information, see Removing Zones.

If you restore deleted zones from the Recycle Bin, the Grid member restores it on the Microsoft server as well. For information, see Restoring Zone Data.

Managing Resource Records in Synchronized Zones

From Grid Manager, you can add and edit resource records in zones served by Microsoft servers. For information about adding and managing resource records, see Managing Resource Records. You can also use IP Map and the IP List to track A, AAAA and PTR records that are synchronized from Microsoft servers. For information, see Chapter 13, IP Address Management.

Microsoft DNS servers support all the resource records supported by Infoblox DNS servers, except for hosts, bulk hosts and shared record groups. You cannot add these records to zones served by Microsoft servers or assign zones with these records to Microsoft servers. Following are guidelines for adding and managing resource records in synchronized zones:

- Infoblox DNS servers support defining a naming policy for the hostnames of A, AAAA, MX, and NS records based on user-defined or default patterns. For information, see Specifying Hostname Policies. The hostname policy applies only when records are created from Grid Manager. Resource records that originate from the Microsoft server are synchronized to the Grid member even if they do not comply with the hostname policy of the Grid member. The policy is enforced only if you edit the resource record from Grid manager.
- When you create an A or AAAA resource record on the NIOS appliance with the option to automatically create the corresponding PTR record, Grid Manager uses the deepest reverse zone that can hold the record. For example, a Grid has the following reverse zones: 10.in-addr.arpa, 0.10.in-addr.arpa, and 0.0.10.in-addr.arpa. When you create the A record www A with the IP address 10.0.0.1, Grid Manager creates a PTR record in the zone 0.0.10.in-addr.arpa. If the deepest zone does not allow the creation of the PTR record, Grid Manager creates the A record, but not the PTR record, and displays a warning.

Note: If the Enable PTR record removal for A/AAAA records option is selected and if you try to delete the A or AAAA records in zones served by Microsoft servers, the appliance displays the Delete Confirmation (A or AAAA Record) dialog box to confirm whether you want to remove the corresponding PTR record that was automatically generated while creating the A or AAAA record. In the Delete Confirmation dialog box, select the Remove associated PTR resource record(s) check box and click Yes to delete the associated PTR record or click No to cancel. For information about enabling this option, see Deleting PTR Records associated with A or AAAA Records.

- You can add and edit DNAME records in a DNS zone assigned to a Microsoft server running Windows 2008 or Windows Server 2012. You cannot add or edit DNAME records in zones assigned to Microsoft servers running earlier Windows versions.
- You can disable synchronized resource records from Grid Manager. When you disable a resource record, it is removed from the Microsoft server at the next synchronization.
- If you add a resource record with invalid data from Grid Manager, such as a DNAME record with an alias name that has special characters, the invalid resource record is not synchronized to the Microsoft server and is eventually deleted from the Grid. The error is logged in the Microsoft log.
- If the zone of the resource record was created using Grid Manager, then it and all its resource records inherit their TTL values from the Grid. Note that these values might be different from those on the Microsoft server. You can change these values to match those on the Microsoft server. For information on changing these values, see Configuring DNS Service Properties.
- Grid Manager and Microsoft DNS servers display TXT records differently. On Grid Manager, you enter the text string of TXT records as defined in RFC 1035. You can enter the following:
  - A contiguous set of characters without spaces. If you enclose the characters in double quotes, Grid Manager displays the character string without the double quotes. For example, if you enter "abcdef", Grid Manager displays abcd ef.
  - A string that contains any character, including spaces, enclosed in quotes.
    - If the string contains a quote ("), you must precede it with a backslash.
    - If you enter a text string with multiple spaces between each word and the string is not enclosed in double quotes, Grid Manager displays the text string with a single space between each word. For example, if you enter text string, the GUI displays text string. To preserve multiple spaces, enclose the string in double quotes.

Unlike on Microsoft DNS servers, you cannot enter a text string on multiple lines in Grid Manager. However, each contiguous set of characters or quoted string entered on Grid Manager is equivalent to a separate line entered on a Microsoft DNS server.

On a Microsoft DNS server, you can enter text without quotes and with each line on a separate line. Microsoft DNS servers then display the text in a brief format where the lines are separated by a comma and a space.

For example, if you enter the following in the Text field of the TXT Record wizard or editor on Grid Manager:

"this is a line""with another line""and a third one"

It is served by the Microsoft and Infoblox DNS servers as:

"this is a line""with another line""and a third one"
But it is displayed in the Microsoft DNS server as:

this is a line, with another line, and a third one

### Synchronizing Updates

A Grid member synchronizes DNS data with each managed Microsoft server at regular intervals. Grid Manager admins with the applicable permissions can then update the synchronized DNS zones and resource records. During each synchronization, updates from Grid Manager are applied to the Microsoft server and updates from the Microsoft server are applied to the Grid as well. Note that the resource records are synchronized only if there is a change to the SOA record on either the Microsoft server or the Grid.

The following examples illustrate how Grid members synchronize DNS data:

- If a Microsoft server admin adds the finance.corpxyz.com zone, it is also added to the Grid after a synchronization.
- If a Grid Manager admin changes the A record of admin.corpxyz.com from 10.2.1.5 to 10.2.1.6, the IP address of its corresponding A record on the Microsoft server is updated to 10.2.1.6.
- If a Grid Manager admin deletes a DNS zone that is assigned to a Microsoft server, the corresponding zone on the Microsoft server is deleted as well in the next synchronization.

Because admins can update DNS data from the Microsoft server and from Grid Manager, conflicts can occur during synchronization. In addition, Microsoft servers and Infoblox DNS servers have some differences in the features they support and the way they handle certain zones and resource records.

The following guidelines describe how the Grid member resolves conflicts and handles any differences when DNS data is synchronized between a Microsoft server and the Grid:

- On Microsoft servers, users can enter FQDNs and labels using a mix of upper and lower case characters. The servers preserve the original case when they store the data. When the Grid member synchronizes data with the Microsoft server, it displays the data in lower case in Grid Manager and the Infoblox API. The case of the data is preserved as long as no change is made to the DNS zone or resource record. If a Grid Manager admin modifies a DNS zone or resource record, the next synchronization converts the object name to lower case on the Microsoft server.
- If a Microsoft server admin modifies an object that has a pending scheduled task and synchronization occurs before the scheduled task, the object is modified in both the Microsoft server and the Grid member. When the scheduled task executes at its scheduled time, it fails and an error message is logged in the audit log.
- A situation could arise where two Microsoft servers in different domains are primary servers for zones with the same name. For example, two reverse-mapping zones could be named 1.1.10.in-addr-arpa in two Microsoft servers managed by the same member. If the two Microsoft servers are synchronized to different DNS views, the Grid member synchronizes each one separately. If the Microsoft servers are synchronized to the same DNS view, then the Grid member synchronizes the zone with the first Microsoft server. During the synchronization with the second Microsoft server, the Grid member logs an error and does not synchronize the zone.
- The Grid member does not synchronize the naming policy configured on Microsoft servers. Zones and resource records that fail the policy check on Microsoft servers are reported in the synchronization log file.
- When you remove a Microsoft server that is assigned to a zone, the succeeding synchronization removes the zone from the Microsoft server.

A situation could arise where two Microsoft servers in different domains are primary servers for zones with the same name. For example, two reverse-mapping zones could be named 1.1.10.in-addr-arpa in two Microsoft servers managed by the same member. If the two Microsoft servers are synchronized to different DNS views, the Grid member synchronizes each one separately. If the Microsoft servers are synchronized to the same DNS view, then the Grid member synchronizes the zone with the first Microsoft server. During the synchronization with the second Microsoft server, the Grid member logs an error and does not synchronize the zone.

The Grid member does not synchronize the naming policy configured on Microsoft servers. Zones and resource records that fail the policy check on Microsoft servers are reported in the synchronization log file.

When you remove a Microsoft server that is assigned to a zone, the succeeding synchronization removes the zone from the Microsoft server.

### Table 35.1

<table>
<thead>
<tr>
<th>Grid Manager Admin...</th>
<th>Microsoft Server Admin...</th>
<th>After Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletes the corpxyz.com zone</td>
<td>Updates the corpxyz.com zone</td>
<td>The corpxyz.com zone is created on the Grid with the updates and is assigned to the Microsoft server.</td>
</tr>
<tr>
<td>Changes the zone transfer settings of the sales.corpxyz.com zone.</td>
<td>Deletes the sales.corpxyz.com zone.</td>
<td>The sales.corpxyz.com is deleted from the Grid as well.</td>
</tr>
</tbody>
</table>

Changing the name or IP address of a resource record on the Microsoft server effectively deletes the original resource record and creates a new record with the current information. During the synchronization, the Grid member also deletes the original record, including its associated properties, such as its extensible attributes and administrative permissions, and creates a new record.

For example, as shown in Figure 35.1, the A record for printer1.corpxyz.com is on both the Microsoft and Infoblox Grid member. On the Grid, the A record has extensible attributes and a comment. A Microsoft server admin changes the IP address of the A1 resource record from 10.1.1.2 to 10.1.1.3. On the Microsoft server, this is equivalent to deleting the A1 resource record with the IP address 10.1.1.2 and then adding a new A1 resource record with the IP address 10.1.1.3. When the data is synchronized, the Grid member deletes the original record with its extensible attributes and comments and creates a new A record with IP address 10.1.1.3.

Figure 35.1
If a Microsoft server admin changes the IP address of a resource record and a Grid Manager admin changes the IP address of the same resource record, they are effectively deleting the record and each creating a new one. For example, as shown in Figure 35.2, a Microsoft server admin changes the IP address of the A resource record for printer1.corpxyz.com from 10.1.1.2 to 10.1.1.3, and a Grid Manager admin changes the IP address of the same resource record to 10.1.1.4. When the data is synchronized, the Grid member deletes the A1 resource record with IP address 10.1.1.2 and creates an A resource record with IP address 10.1.1.3 and another A1 resource record with IP address 10.1.1.4.
The Microsoft server does not allow the creation of arpa subzones as forward-mapping zones, similarly, the appliance restricts assigning arpa subzones (zone names ending with .arpa) to the Microsoft server.

NIOS does not synchronize the top-level reverse-mapping zones (in-addr.arpa and ip6.arpa) created on the Microsoft server and the top-level reverse-mapping zones (in-addr.arpa and ip6.arpa) created on the NIOS appliance cannot be assigned to the Microsoft server.

Grid members can synchronize classless IPv4 reverse-mapping zones from the Microsoft server to the Grid only if the zone prefix is in one of the following formats: <subnet>/<subnet mask bit count> or <subnet>-<subnet mask bit count>. For example, 128/26.2.0.192.in-addr.arpa. If the zone prefix is not in the specified format, the Grid member skips the zone and logs an error message. For information, see http://technet.microsoft.com/en-us/library/cc961414.aspx. Likewise, Grid Manager admins can add a classless IPv4 reverse-mapping authoritative or stub zone to a Microsoft server only if its prefix is in the specified format. For information about configuring classless IPv4 reverse-mapping zones in Grid Manager, see Specifying an RFC 2317 Prefix.

Grid members synchronize DNS records that contain values that Infoblox does not support. Grid Manager admins can view these records, but they cannot edit or restore such records. For example, if a member synchronizes a NAPTR record that contains an unsupported value in the Service field, admins can view this record but they cannot edit or restore it, as long as it contains an unsupported value.

When a Grid member synchronizes a zone from a Microsoft server to the appliance and that zone contains UTF-8 characters in the “Responsible Person” field, Grid Manager displays the “Responsible Person” value in the RNAME field of the SOA record of the zone. Note though that you cannot edit the SOA record if the FNAME field contains unsupported UTF-8 characters.

Synchronizing Delegations

When a parent zone delegates a subdomain to one or more name servers, Infoblox DNS servers require the delegation name servers to also be authoritative for the subzone. Microsoft servers do not; they allow the delegation servers of a subzone to be different from its authoritative servers. Infoblox DNS servers support this configuration only if the primary server of the parent zone is a Microsoft server. This configuration is retained when delegations are synchronized from Microsoft servers to the Grid.

For example, as shown in Figure 35.3, on a Microsoft server, corpxyz.com delegates sales.corpxyz.com to the name server ns1.corpxyz.com; but the authoritative server of sales.corpxyz.com is 2k3r264-2.infoblox.com. Figure 35.3 Delegation Server and Authoritative Server for corpxyz.com
Figure 35.4 shows that after corpxyz.com and its subzone are synchronized to the Grid, corpxyz.com contains an NS record for sales.corpxyz.com and an A record for the delegation name server ns1.corpxyz.com. The MS Delegation Addresses column displays the IP address of the delegation server of the subzone sales.corpxyz.com.

After the synchronization, you can add name servers for the delegation as follows:

1. Select the zone by navigating to the Data Management tab -> DNS -> Zones -> parent_zone.
2. Click the Add icon and select Record -> NS Record.
3. Complete the following and click Next:
   - **Name Server**: Enter the hostname you want to configure as the name server for the zone.
   - **Name**: Specify the name of the subzone. Note that you cannot change this name when you edit the record.
4. Enter the IP address of the name server.
5. Save the configuration.

NIOS adds an NS record for the new delegation server and synchronizes this update to the Microsoft server. In Figure 35.5, a new delegation server, ns2.corpxyz.com, was added.

When you navigate to the Name Servers tab of sales.corpxyz.com to view the authoritative name servers for the subzone, note that as shown in Figure 35.6, the table displays 2k8r264-2.infoblox.com as the authoritative server for the subzone. The Parent Delegation column indicates if the
FQDN and IP address of the authoritative name server for the zone matches the FQDN and IP address in the delegation zone's NS record. In the example, the authoritative name server 2k8r264-2.infoblox.com is different from the delegation name servers (ns1.corpxyz.com and ns2.corpxyz.com), so the column displays **No**.

*Figure 35.6 Authoritative Name Server of sales.corpxyz.com*

Note though that because Infoblox DNS servers require the delegation servers to also be authoritative for the subzone, if you add another authoritative name server to the subzone from Grid Manager, NIOS also adds it as a delegation server in the parent zone. For example, as shown in *Figure 35.7*, when an admin adds the name server ns-100.corpxyz.com as an external secondary server for sales.corpxyz.com, NIOS automatically adds it as a delegation server by adding an NS record for it in the parent zone.

*Figure 35.7 Adding Another Authoritative Server from Grid Manager*
Synchronizing AD-Integrated Zones

An AD-integrated zone can be served by multiple domain controllers, and a Grid member can manage more than one of the domain controllers. If the domain controllers are configured to synchronize their DNS data to different DNS views, the Grid member synchronizes DNS data with each domain controller. If the domain controllers are configured to synchronize their DNS data to the same DNS view, the member selects a principal server for synchronization purposes and synchronizes data with that principal server only. The selection of the principal server is logged, as well as when it changes. The Grid member selects a principal server as follows:

- The first domain controller that is assigned as the primary server is designated principal server.
- If a domain controller fails three successive synchronizations, it loses its principal status. The Grid Master then checks the date that each domain controller last became a principal server and selects the one that has not been the designated principal the longest.
- If the domain controllers are managed in read-only and read/write modes, the Grid member always selects the domain controller that is managed in read/write mode.

When a zone is served by multiple Microsoft servers, the **MS Sync Server** column of the **Zones** tab shows which Microsoft server is actually performing the synchronization of that zone with the Grid.

The Grid member periodically checks if each zone has one principal server. If it does not find a principal server for a zone, the Grid member selects one among the name servers assigned to the zone. It gives priority to the server that was not the designated principal server the longest.

Following are additional guidelines when synchronizing AD-integrated zones:

- You can create an AD-integrated zone on Grid Manager and assign one domain controller as its primary server. If a domain controller admin adds more primary servers to the zone, they are added to the zone on Grid Manager when the zone is synchronized. If you want to delete the primary servers, you must delete all the primary servers at once. You cannot delete only a subset of the servers.
- A situation could arise where two domain controllers in different AD domains are primary servers for zones with the same name. For example, two reverse-mapping zones could be named 1.1.10.in-addr-arpa in two domain controllers managed by the same member. If the two domain controllers are synchronized to different DNS views, the Grid member synchronizes each one separately. If the domain controllers are synchronized to the same DNS view, then the Grid member synchronizes the zone with the first domain controller. During the synchronization with the second domain controller, the Grid member logs an error and does not synchronize the zone.
• If a Grid Manager admin deletes a CNAME record that has a blank canonical name from an AD-integrated zone, this CNAME record is not deleted from the Microsoft server after the synchronization if the AD-integrated zone is hosted on a Microsoft server running Windows 2008 R2 or Windows Server 2012.
• When a Microsoft server is the primary server of a zone that contains an _msdcs zone, it appends the parent zone name to the server name in the NS record of the _msdcs zone. When an Infoblox Grid member is the primary server of a zone that contains an _msdcs zone, it specifies the server name only in the NS record. For example, the _msdcs zone is in the corpxyz.com zone and the name server is nameserver100.com. When a Microsoft server is the primary server of corpxyz.com, the server name on the NS record of the _msdcs zone is nameserver100.corpxyz.com. When a Grid member is the primary server, the server name on the NS record of the _msdcs zone is nameserver100.com.

Resolving Conflicts

Some conflicts require intervention from an admin. For example, a Grid member cannot synchronize a zone when its primary server on the Microsoft server is different from its primary server on the Grid. When a Grid member is unable to synchronize data due to such conflicts, it logs an error, skips the object with the error and continues synchronizing the rest of the data. You can then view the Microsoft logs to check which objects were not synchronized. If you resolve the problem, the Grid member synchronizes the object on its next attempt. For information about the logs, see Viewing Synchronization Logs.

Viewing Members and Managed Servers

You can view Infoblox and Microsoft DNS servers by navigating to the Data Management tab -> DNS tab, and then selecting the Members/Servers tab. The panel displays the following information about each DNS server:

- **Name**: The hostname of the Grid member or Microsoft server.
- **Status**: The status of the DNS service on the Grid member or Microsoft server.
- **Comment**: Comments that were entered for the Grid member or Microsoft server.
- **Site**: Values that were entered for this pre-defined attribute.
- **Address**: The IP address of the Grid member or Microsoft server. You can do the following:
  - List the DNS views or zones served by the member or Microsoft server.
  - Click a Grid member or Microsoft server name.
  - Edit the properties of a Grid member or Microsoft server.
    - Click the check box beside a Grid member or Microsoft server, and then click the Edit icon. To edit the DNS properties of a Grid member, see Configuring DNS Service Properties. To edit the DNS properties of a Microsoft server, see Specifying Forwarders for Microsoft Servers.
    - Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
    - Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
  - Export the list of Grid members and Microsoft servers to a .csv file.
    - Click the Export icon.
  - Print the list of Grid members and Microsoft servers.
    - Click the Print icon.

Specifying Forwarders for Microsoft Servers

A forwarder is a name server to which all other name servers first send queries that they cannot resolve locally. The forwarder then sends these queries to DNS servers that are external to the network, avoiding the need for the other name servers in your network to send queries off-site.

You can define a list of forwarders for each managed Microsoft server as follows:

1. From the Data Management tab, select the DNS tab -> Members/Servers tab -> ms_server check box -> Edit icon.
2. Click the Add icon and enter the IP address of the forwarder in the text field.
3. Save the configuration and click Restart if it appears at the top of the screen.

Disabling and Removing Microsoft DNS Servers

When you disable synchronization with a Microsoft server, the managing Grid member completes any ongoing synchronization and does not start a new one. Synchronization resumes when the Microsoft server is re-enabled. The synchronized DNS data stays in the same state until synchronization resumes. For information, see Disabling Synchronization.

When you remove a managed Microsoft server from the Grid, the managing Grid member terminates any ongoing synchronization and does not start a new one. Zones and their content on the Microsoft server remain in the state that existed the moment the Microsoft server was removed. The Grid retains the zones that were assigned to the Microsoft server that was removed, but deletes the Microsoft server from its assigned zones as follows:

- If the Microsoft server is the only primary server and there are no other assigned servers or if the secondary server is an external secondary server, Grid Manager deletes all the server assignments.
- If the Microsoft server is the only primary server and there are Grid secondary servers, an external primary is created with the FQDN and IP address of the removed Microsoft server.
- If the Microsoft server is a secondary server and there is a Grid primary, an external secondary is created with the FQDN and IP address of the removed Microsoft server.
1. If the Microsoft server is a server for a stub zone, the server is removed. To remove a Microsoft DNS server:

   From the **Data Management** tab, select the **DNS tab -> Members/Servers** tab -> **ms_server** check box.
   2. Expand the Toolbar and click **Delete**.
   3. Click **Yes** when the confirmation dialog box appears.

### Chapter 36 Managing Microsoft DHCP Services

This chapter provides guidelines for using Grid Manager to manage Microsoft DHCP servers and for synchronizing DHCP data between Microsoft servers and the Grid. It discusses some features of the Microsoft DHCP servers only as they relate to the synchronization of data. Please review the Microsoft documentation for complete information about Microsoft DHCP servers and their features.

In addition, if you encounter technical issues with your Microsoft DHCP servers, contact Microsoft Technical Support or consult the Microsoft Support site at [http://support.microsoft.com/](http://support.microsoft.com/). Some Windows versions require certain updates and hotfixes installed, so the Microsoft server can synchronize with the Grid member. For information about these requirements, see **Requirements**.

The topics in this chapter include:

- **About Microsoft DHCP Management**
  - Synchronizing DHCP Data from Microsoft Servers
  - Viewing Synchronized Leases
- **Synchronizing DHCP Failover Relationships**
  - About Microsoft DHCP Failover Relationships
  - Admin Permissions for Managing Microsoft DHCP Failover Relationship
  - Admin Permissions for Managing Failover Relationships for DHCP Ranges
- **Synchronizing IP Addresses with Invalid MAC Addresses**
- **Managing Synchronized DHCP Data**
  - Adding and Managing Scopes
  - Viewing Scopes
  - Adding Fixed Addresses/Microsoft Reservations
  - About Superscopes
  - Synchronizing Updates
- **Managing Microsoft DHCP Servers**
  - Viewing Members and Managed DHCP Servers
  - Setting Microsoft DHCP Server Properties
  - Controlling the DHCP Service of a Microsoft Server
  - Disabling and Removing Microsoft DHCP Servers
  - Modifying DHCP Server Assignments

#### About Microsoft DHCP Management

Grid Manager enables you to centrally manage the DHCP data of multiple Microsoft DHCP servers from a single interface. Once the DHCP data is synchronized, you can use the Dashboard on Grid Manager to monitor DHCP and server operations, or organize DHCP data into Smart Folders. Through IPAM tools, such as network maps and IP maps, you can track and manage IP address usage in your networks and monitor DHCP range utilization. You can also run a network discovery to retrieve IP allocation for both managed and unmanaged devices—including virtualized resources. For information about the IPAM features, see Chapter 13, **IP Address Management**.

*Figure 36.1 Managing Microsoft DHCP Servers from Grid Manager*
Synchronizing DHCP Data from Microsoft Servers

After you configure a member to manage the DHCP service of a Microsoft server, the Grid member connects to the server and starts synchronizing IPv4 DHCP data from the Microsoft server to the Grid database. It synchronizes the Microsoft server properties, leases, scopes and reservations. The synchronization time varies, depending on different factors, such as the number of managed Microsoft servers and the amount of data being synchronized.

Note: Synchronizing IPv6 data is not supported.

As shown in Table 36.1, Microsoft servers and Infoblox DHCP servers represent DHCP data differently. Scopes on Microsoft servers are DHCP ranges on Infoblox DHCP servers. Additionally, Microsoft servers support split-scopes, which is a scope assigned to two Microsoft servers. Each scope has an exclusion range on opposite ends to specify the pool of IP addresses that the other Microsoft server allocates. On an Infoblox DHCP server, each scope in the split-scope is represented as a DHCP range with an exclusion range. Note that NIOS also synchronizes scopes assigned to more than two Microsoft servers, but they are not synchronized as split-scopes. Fixed addresses on Infoblox DHCP servers are the same as reservations on Microsoft servers. Infoblox reservations, which are IP addresses that are excluded from DHCP, are not supported on Microsoft servers. Microsoft superscopes, which are used to group scopes, are represented as superscopes and can be managed from Infoblox DHCP servers.

Table 36.1 DHCP Data in Microsoft and Infoblox DHCP Servers

<table>
<thead>
<tr>
<th>DHCP Data</th>
<th>Microsoft DHCP Servers</th>
<th>Infoblox DHCP Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address pool from which the server allocates addresses</td>
<td>Scope</td>
<td>DHCP Address Range in a Network</td>
</tr>
<tr>
<td>An IP address that is always assigned to the same device</td>
<td>Reservation</td>
<td>Fixed Address</td>
</tr>
<tr>
<td>An IP address that is excluded from DHCP because a user intends to configure it manually on a network device</td>
<td>Not supported</td>
<td>Reservation</td>
</tr>
<tr>
<td>Administrative group of scopes</td>
<td>Superscope</td>
<td>Microsoft superscope</td>
</tr>
</tbody>
</table>

Note: In this chapter, reservations always refer to Microsoft reservations (Infoblox fixed addresses), unless otherwise specified.

When the member synchronizes a scope to the Grid, it converts the scope to a DHCP range and network. For example, it converts the Microsoft scope 10.1.1.1-10.1.1.200 with a netmask of /24 to the network 10.1.1.0/24 and DHCP range 10.1.1.1-10.1.1.200 on Grid Manager. The member associates the DHCP properties of the scope, including its DHCP and Microsoft vendor options, with the DHCP range. It synchronizes the leases within the range and if configured, the exclusion range as well. NIOS synchronizes two scopes as split-scopes if the following conditions are met:

- Two scopes have the same address range.
- The scopes are assigned to two different Microsoft servers.
- Each scope has an exclusion range and the exclusion ranges are at opposite ends of the scope, so they complement each other. For example, the scope 10.1.1.1-10.1.1.200 on Microsoft server A has an exclusion range of 10.1.1.100-10.1.1.200 and the same scope on Microsoft server B has an exclusion range of 10.1.1.1-10.1.1.99.

When the appliance synchronizes a split-scope, it sets a split-scope flag on each scope to indicate that it is part of a split-scope. For more information, see Viewing Scopes. It synchronizes any reservations that are configured in each scope as well. When the member synchronizes a Microsoft reservation to the Grid, it converts the reservation to a fixed address and static lease on Grid Manager. It associates the DHCP properties and DHCP and Microsoft vendor options of the reservation with the fixed address record. The Grid member synchronizes superscopes to the Grid as well. The Grid supports Microsoft superscopes, when an MS management license is installed. For information about adding and managing superscopes in Infoblox DHCP servers, see About Superscopes.

Following are some guidelines on how a Grid member synchronizes DHCP data from Microsoft servers to the Grid:

- If two superscopes have the same name, but are served by different servers, the member creates two different superscopes on the Grid, each appended with the Microsoft server FQDN.
- The member synchronizes all active and inactive scopes from a managed Microsoft server as long as the scopes do not conflict or include any networks currently served by a Grid member. The member does not synchronize a scope if its network already exists in the Grid and is served by a Grid member. It can synchronize a scope if its network is included in an existing network, only if the network is not served by DHCP.
- Synchronizing scopes that are larger than /12 is not supported.
- NIOS synchronizes all scopes except for those with serving ranges that overlap the serving ranges of existing DHCP ranges.
- If the appliance manages multiple Microsoft servers and synchronizes identical scopes from more than two Microsoft servers, it does not flag the scopes as split-scopes.
- If the appliance synchronizes one or more scopes from Microsoft servers that are identical to an existing split-scope, it removes the split-scope flag from the existing split-scope.
- NIOS does not synchronize partially overlapping scopes inside a single network from different Microsoft servers. It synchronizes only
ranges that completely overlap.
• More than two scopes are not synchronized as split-scopes, even if they are identical and have exclusion ranges that complement each other.
• Scopes that have more than one exclusion range are not synchronized as split-scopes, even if the exclusion ranges complement each other. In addition, if a split-scope is synchronized from a Microsoft server and one of the scopes is split again on the Microsoft server, NIOS synchronizes the third scope, but does not set a split-scope flag. In addition, it removes the split-scope flag from the original split-scopes.

You can view the synchronized data as follows:

• To view the networks of the scopes, select the Data Management tab -> DHCP tab -> Networks tab -> Networks panel. This panel displays all IPv4 networks. For information about this panel, see Modifying IPv4 Networks.
• To view the corresponding DHCP ranges and reservations, select the Data Management tab -> DHCP tab -> Networks tab, and click a network link. For information about this panel, see Viewing Scopes.

You can also use the features in the IPAM tab, such as the Net Map and IP Map, to view and manage the Microsoft DHCP data. For information, see Chapter 13, IP Address Management.

Viewing Synchronized Leases

A Grid member synchronizes all leases from its managed Microsoft server to the Grid. Microsoft servers automatically generate a static lease for each reservation. These static leases are synchronized to the Grid as well. You can view the synchronized leases by navigating to the Data Management -> DHCP -> Leases tab. For information about viewing current leases, see Viewing Current Leases. You can do the following:

• View lease details, by selecting a lease and clicking the Lease Details icon. For additional information, see Viewing Detailed Lease Information.
• Clear a lease, by selecting it and clicking the Clear Lease icon. Note that Grid Manager clears the lease immediately. It does not wait for the next synchronization.
• Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
• Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.

Additionally, you can enable a Grid member to log lease related operations, so you can view these events in the Lease History panel. For information, see Configuring the Lease Logging Member and Viewing Lease History.

Synchronizing DHCP Failover Relationships

The synchronization of DHCP data with Microsoft DHCP servers running Microsoft Windows version 2012 or later includes the synchronization of DHCP failover relationships and the associated scopes. Note that this feature does not have any impact on the synchronized data with Microsoft servers running a Windows version earlier than 2012.

When you change the synchronization mode of a Microsoft server, it affects the way a failover relationship is synchronized and replicated, but you cannot change these settings directly. When a failover relationship synchronization mode changes from read-only to read/write, NIOS copies the DHCP configuration within the relationship between both partners, using the primary Microsoft server as the reference. When a failover relationship synchronization mode changes from read/write to read-only, NIOS does not change the DHCP configuration within the relationship on each Microsoft server.

About Microsoft DHCP Failover Relationships

A failover relationship represents the relationship between two Microsoft DHCP servers, where each of them is called a partner. A failover relationship that has at least one Grid member as a partner is called a NIOS failover relationship and if it has at least one Microsoft server as a partner, it is defined as a Microsoft failover relationship. A failover relationship can be configured with two Microsoft servers, a Microsoft server and an external server, two Grid members, a Grid member and an external server.

When you synchronize a failover relationship from a Microsoft server, the NIOS appliance copies the changes originating from the Microsoft server to the failover relationship of the partner, only if the two Microsoft servers match. Two failover relationships match if they have the same name, and if the address of the partner defined in one Microsoft server matches with the address of the other, and vice versa. Also, you must configure Microsoft servers to manage DHCP and enable synchronization on both the Microsoft servers.

The changes that originate from the Microsoft server are applied to the failover relationship on NIOS, and vice versa. The changes are effective on the partner server from its next scheduled synchronization.

The failover relationship synchronization mode for Microsoft is read/write if both partners are each Microsoft servers that are enabled for DHCP synchronization. For all other cases, the failover relationship synchronization is read only.

When NIOS fails to match a failover relationship, the partner of that relationship is considered to be unknown or external. In the case of multiple servers, you must define the Microsoft server on the appliance using the same IP and/or FQDN.

Infoblox recommends that you do the following for Microsoft servers in a failover relationship:

• The synchronization interval of two Microsoft servers in a failover relationship must be identical and small.
• Use the same managing member for Microsoft servers in a failover relationship.
• After a Microsoft server fails, you must turn off NIOS synchronization during restore to avoid transferring the old configuration to its partners.
• The primary and secondary Microsoft servers that you select in a failover relationship must be in the same network view. Note the following if the servers are on different network views:
  • You cannot modify or delete failover associations.
  • You cannot add, modify, or delete scopes that are associated with the failover association.
• The appliance does not display the FQDN, but displays the IP address and status as 'unknown' for the secondary Microsoft server.
• The appliance may not display the scopes that are assigned to the failover association.
• The appliance does not allow you to perform any action on the objects in a failover association, as the objects will be in read-only mode.

Admin Permissions for Managing Microsoft DHCP Failover Relationship

To create, modify or delete a Microsoft failover relationship in NIOS, you must have the same permissions on both the Microsoft servers that are assigned to the failover relationship. You can update the property of a failover relationship only if it has read/write permissions. You cannot update the properties of the Microsoft server or partner directly. You must first delete the relationship, create a new relationship and assign the DHCP scope to the new relationship. NIOS applies the changes to both Microsoft servers defined in the failover relationship during its next synchronization schedule, only if they are in read/write mode during that time. You can delete a Microsoft failover relationship only if it is not associated with a DHCP range.

Microsoft Failover Relationships for DHCP Ranges

When you create or update a DHCP range on NIOS, administrators can assign or remove a DHCP range from a Microsoft failover relationship only if the failover relationship has two read/write Microsoft servers. Note that when you reassign a DHCP range that is assigned to a Microsoft failover relationship, NIOS removes the DHCP range from the failover relationship during the next synchronization of the respective server.

When you remove a DHCP range from a read/write Microsoft failover relationship, NIOS deletes a copy of the DHCP range from both the Microsoft servers defined in the failover relationship. When a DHCP range is associated with a Microsoft failover relationship, any change made to one copy of the range is automatically saved to the other copy.

Admin Permissions for Managing Failover Relationships for DHCP Ranges

You must have read/write permissions on the DHCP range and on each Microsoft server to assign or remove a DHCP range from a Microsoft failover relationship. Note that the changes performed on a DHCP range, which is assigned to a read/write Microsoft failover relationship, are applied to both copies of the range and synchronized with each Microsoft server during each of their next scheduled synchronization.

You can delete a DHCP range that is assigned to a Microsoft failover relationship only if the failover relationship has two read/write Microsoft servers. When you delete a DHCP range that is assigned to a Microsoft failover relationship in read/write mode, NIOS deletes them on both Microsoft servers that is defined in the relationship during the next respective scheduled synchronization.

Limitations of Microsoft DHCP Failover Relationship on NIOS

Note the following limitations of Microsoft DHCP failover relationship on NIOS:

1. You cannot synchronize failover scope statistics on a Microsoft DHCP failover relationship.
2. The appliance does not support on demand replication for a Microsoft DHCP failover relationship.
3. You cannot set the functional peer in the PARTNER-DOWN state for a Microsoft DHCP failover on NIOS. For information, see Setting a Peer in the Partner-Down State.
4. The appliance does not support time synchronization of both partners and time synchronization monitoring. Infoblox recommends that the administrators of the Microsoft servers running the DHCP server must ensure that the time synchronization is appropriate.
5. You can only add up to 31 DHCP failovers to a Microsoft server in a failover relationship.

Synchronizing IP Addresses with Invalid MAC Addresses

An invalid MAC address is a MAC address whose length is not six bytes (48 bits). You can synchronize IP addresses with invalid MAC addresses only for Microsoft servers for which you have enabled DHCP synchronization. When you enable this setting for a Microsoft DHCP server, NIOS synchronizes any DHCP lease or reservation with an invalid MAC address and it is effective from the next scheduled DHCP lease or DHCP server synchronization. The synchronization does not affect a DHCP lease or reservation with a valid MAC address.

You can synchronize IP addresses with invalid MAC addresses at the Grid level and override them at the member level. This is valid for NIOS 6.11.0 and later releases. The appliance displays the invalid MAC address using a red cross mark in the list. You cannot save invalid MAC addresses, but you can view invalid MAC addresses in the list panels and editors.

When you disable synchronization for invalid MAC addresses, NIOS ignores any DHCP lease or reservation with an invalid MAC address and the object disappears from NIOS during the next synchronization of the Microsoft server to which it belongs. An invalid MAC address that you had synchronized earlier persists until NIOS updates the associated lease or reservation with a new MAC address, or the lease is cleared, or deleted, or expired.

To synchronize an invalid MAC address, complete the following:

1. **Grid:** From the Grid tab -> Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit.
   **Member:** From the Grid tab -> Grid Manager tab, click the Members tab, select the member check box, and click the Edit icon.
2. Select the Microsoft Server Settings tab in the Grid Properties Editor wizard and complete the following in the Advanced tab:
   • Allow Invalid MAC Address to be synchronized: This is enabled, by default. Select this to enable synchronization for invalid
MAC addresses.
You can click Override at the member level to specify a new value. The Override button changes to Inherit. Click Inherit to inherit the value from the Grid.

3. Save the configuration.

Managing Synchronized DHCP Data

When Grid members are configured to manage Microsoft DHCP servers in read/write mode, you can use Grid Manager to view, edit and delete the DHCP data of those servers. You can add and manage networks and DHCP ranges that are synchronized as scopes to the Microsoft server, and add and manage reservations and superscopes. All updates are synchronized to the Microsoft servers at regular intervals.

Grid Manager also allows you to set admin permissions, extensible attributes, and thresholds. These apply only when the DHCP data is managed on Grid Manager. These properties are not synchronized to Microsoft servers.

The following sections provide guidelines for managing Microsoft DHCP data from Grid Manager:

- 5800935
- 5800935
- 5800935

Adding and Managing Scopes

To add a scope from Grid Manager, you must create an IPv4 network and a DHCP range, and then assign the Microsoft server to the network and range. To add a split-scope from Grid Manager, you must create an IPv4 network and a DHCP range, and then assign two Microsoft server to the network and range.

To edit a scope synchronized from a Microsoft server, you must edit the properties of its corresponding DHCP range. The following sections describe how to add, edit and remove scopes using Grid Manager.

Note: Microsoft servers do not support Infoblox hosts and reservations. You cannot add them to networks and DHCP ranges served by Microsoft servers.

Adding Networks for Scopes

Following are guidelines for adding a network for Microsoft scopes:

- The network must be served by Microsoft servers. It cannot be served by a mix of Microsoft and Infoblox DHCP servers.
- If you are adding a split-scope, you must assign the network to two Microsoft servers that serve the split-scope. A split-scope cannot be served by a mix of Microsoft and Infoblox DHCP servers.
- The network can contain only one DHCP range per Microsoft server. It can contain multiple DHCP ranges as long as they do not overlap and are each served by a different Microsoft server.
- You can set DHCP properties at the DHCP range level only, not the network level.

You can run discoveries on networks served by Microsoft servers. For information about network discoveries, see IP Discovery and vDiscovery.

Note: Networks served by Microsoft DHCP servers do not support the split, join, and expand functions.

You can create a network from scratch or use a network template. For information about creating network templates, see Adding IPv4 Network Templates. To add an IPv4 network for a scope:

1. From the Data Management tab, select the DHCP tab.
2. If you have more than one network view in the system, select the network view in which you want to add the network. It must be the same network view to which the Microsoft server is assigned.
3. Expand the Toolbar and click Add > Network.
4. In the Add Network wizard, select one of the following and click Next:
   - Add Network
   - Add Network using Template: Click Select Template and select a network template. For more information, see About IPv4 Network Templates. In the DHCP Network Template Selector dialog box, select the template you want to use and click the Select icon. Note that when you use a template to create a network, the configurations of the template apply to the new network. The appliance populates the template properties in the wizard when you click Next. You can then edit the pre-populated properties, except for Netmask.
5. Complete the following and click Next:
   - Address: Enter the IP address of the network. You can enter the IP address with a CIDR block. For example, enter 10.0.0.0/24, and the netmask slider adjusts the netmask to /24. You can also enter partial IP address with a CIDR block. When you are done, Grid Manager displays the complete IP address with the CIDR block. For example, when you enter 15/24, Grid Manager displays 15.0.0.0/24 and the netmask slider adjusts the netmask to /24. Note that Microsoft DHCP servers do not support /32 subnets.
   - Netmask: Use the netmask slider to select the appropriate number of subnet mask bits for the network. Microsoft servers support /1 to /31 netmasks. Note that when you use a template that contains a fixed netmask, you cannot adjust the netmask for...
Setting Network Properties

You can change the Microsoft servers assigned to the network, and define extensible attributes and admin permissions to the network. You can also set thresholds for the network, to enable the appliance to make a syslog entry when address usage goes above or below the thresholds. To set network properties:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.
2. The Network editor contains the following basic tabs from which you can modify data:
   - **General Basic**: You can enter or modify comments.
   - **Member Assignment**: Add or delete Microsoft servers. For information, see Adding IPv4 Networks. If the network contains multiple DHCP ranges each managed by a different Microsoft server, then you can add those Microsoft servers here.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with a specific network. You can also modify the values of the extensible attributes. For information, see About Extensible Attributes.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions.
3. Optionally, you can click **Toggle Expert Mode** to display the following tabs from which you can modify advanced data.
   - **General Advanced**: You can associate zones with a network. For information, see Associating Networks with Zones.
   - **Thresholds**: These watermarks represent thresholds above or below which address usage is unexpected and might warrant your attention. Thresholds are inherited from the Grid.
     - **High-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range exceeds this number, the appliance makes a syslog entry. The default is 95.
     - **Low-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range drops below this number, the appliance makes a syslog entry. The default is 0. Address usage must initially exceed the low-water mark threshold and then dip below it before the appliance considers low address usage an event requiring an alert.
4. Save the configuration and click Restart if it appears at the top of the screen.

Deleting and Restoring a Network

When you delete a network, Grid Manager moves it and its DHCP ranges and fixed addresses to the Recycle Bin, and permanently deletes its leases. The corresponding scopes and reservations are deleted from the Microsoft server at the next synchronization. If you restore the network on Grid Manager, its DHCP ranges and fixed addresses are restored as well. The Grid member then adds the corresponding scopes and reservations to the Microsoft server on the next synchronization. For information about deleting networks, see Deleting IPv4 Networks. For information about restoring data, see Using the Recycle Bin.

Adding a DHCP Range/Scope

After you add a network for a scope, you must then define its DHCP range. You can create the DHCP range from scratch or use a DHCP Range template. For information about DHCP templates, see About IPv4 Range Templates.

You can add multiple ranges to the same network, as long as each range is served by a different Microsoft server and the ranges do not overlap. When you add a split-scope, you must specify the Microsoft servers that serve the scopes and their exclusion ranges. Each scope inherits its...
To add a DHCP range for a scope:

1. From the Data Management tab, select the DHCP tab.
2. Navigate to the network to which you want to add a DHCP range, and then click Add -> DHCP Range from the Toolbar. You can also add a DHCP range from any panel in the DHCP tab.
3. In the Add Range wizard, select one of the following and click Next:
   - Add DHCP Range
   - Add DHCP Range using Template

Click Select Template and select the template that you want to use. Note that when you use a template to create a DHCP range, the configurations of the template apply to the new range. The appliance automatically populates the DHCP range properties in the wizard. You can then edit the pre-populated properties.

4. Complete the following:
   - **Network**: Click Select Network to select the network to which you want to add the DHCP range. The network must be served by a Microsoft server. If you are adding a DHCP range while viewing the contents of a specific network, the appliance displays the network address here. You can still select a different network by clicking Select Network.
   - **Start**: Enter the first IP address in the range.
   - **End**: Enter the last IP address in the range.
   - **Name**: You can enter a name for the DHCP range.
   - **Comment**: You can enter additional information. After the range is synchronized to the Microsoft server as a scope, this text appears in the Description field of the scope on the Microsoft server.
   - **Disable for DHCP**: Select this if you do not want the DHCP server to allocate IP addresses from this DHCP range at this time. If you select this, the Grid member synchronizes the range to the Microsoft server as an inactive scope.
5. Click Next and select one of the following to provide DHCP services for the DHCP range:
   - **None**: Select this if you do not want to synchronize this range to the Microsoft DHCP server.
   - **Microsoft Server**: This field displays the Microsoft server that you selected for the network. If several servers were assigned to the network, you can select one from the list.
     - **Microsoft Split-Scope**: Select this to create a split-scope, and then complete the following:
     - **Microsoft Server #1**: Read-only field that displays the Microsoft server that you specified in the preceding step.
     - **Microsoft Server #2**: Select the Microsoft server that will serve the split-scope.
     - **Split Percentage**: Specify the percentage of IP addresses in the scope that is allocated to the exclusion range of each Microsoft server. The default is 50%. You can either move the slider or enter the percentages in the text fields. When you use the slider, you are specifying the percentage of addresses in the exclusion range of the first server. A tooltip window displays the percentage as you adjust the slider. When you set the split percentages, these fields automatically display the starting address of the exclusion range of each Microsoft server. Alternatively, you can enter the starting address of the exclusion range of the first Microsoft server, and the **Split Percentage** and **Exclusion Starting Address** values adjust accordingly.
     - **Exclusion Starting Address**: When you set the split percentages, these fields automatically display the starting address of the exclusion range of each Microsoft server. Alternatively, you can enter the starting address of the exclusion range of the first Microsoft server, and the **Exclusion Ending Address** values adjust accordingly.
   - **Exclusion Ending Range**: When you set the split percentage, these fields automatically display the ending address of the exclusion range of each Microsoft server. Alternatively, you can enter the ending address of the exclusion range of the second Microsoft server, and the **Exclusion Percentage** and **Exclusion Starting Address** values adjust accordingly.
6. Click Next, and optionally set operational parameters for the scope. Otherwise, the scope inherits its parameters from the first Microsoft DHCP server.
   - **Lease Time**: Specify the lease time. The default is 8 days. When the range is served by a Microsoft server and you enter a lease time of 1000 days or more, Grid Manager automatically grays out this field and checks the Unlimited Lease Time option after you save your entries.
   - **Unlimited Lease Time**: Select this option to set an infinite lease time for the IP addresses leased from this range.
   - **Routers**: In the table, enter the IP address of the router that is connected to the same network as the DHCP clients. Click the Add icon to add more routers.
   - **Domain Name**: Enter the name of the domain for which the Microsoft server serves DHCP data. The DHCP server includes this domain name in Option 15 when it responds with a DHCPOFFER packet to a DHCPOFFER packet from a client.
   - **DNS Servers**: In the table, enter the IP address of the DNS server to which the DHCP clients send name resolution requests. The DHCP server includes this information in the DHCPOFFER and DHCPACK messages.
   - **Broadcast Address**: Enter the broadcast IP address of the network to which the DHCP server is attached.
7. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see Using Extensible Attributes.
8. Save the configuration and click Restart if it appears at the top of the screen.
   
   Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For
Setting DHCP Range/Scope Properties

A Microsoft scope inherits its properties from its Microsoft server. In Grid Manager, you can override the inherited values or set other properties by editing the DHCP range. You can also configure an exclusion range within the scope and set thresholds, to enable the appliance to make a syslog entry when address usage goes above or below the thresholds.

You can modify a scope’s properties, including its start and end addresses, servers, and exclusion ranges. If you edit the properties of a split-scope and it results in gaps or overlapping exclusion ranges so that the ranges are no longer identical, Grid Manager displays a warning indicating that continuing with the operation automatically removes the split-scope flag. Grid Manager also removes the flag when the start or end address of a scope changes, so its range is no longer the same.

To set DHCP range properties:

1. From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.
2. The DHCP Range editor contains the following basic tabs from which you can modify data:
   - **General**: Modify the fields, including the start and end addresses, as described in 5800935 5800935
   - **Server Assignment**: Switch to None or select a different Microsoft server for the DHCP range.
   - **IPv4 DHCP Options**: Keep the DHCP properties or override them and enter unique settings for the DHCP range. For information about the fields, see 5800935.
     - This tab displays DHCP and Microsoft vendor options that were synchronized from the Microsoft server. You can edit any of the options. When you select a different User Class or Vendor Class from the drop-down menus, Grid Manager automatically updates the option definitions in the drop-down list.
     - To configure additional DHCP options, click + and select a User Class and Vendor Class from the drop-down menus. Select an option from the drop-down list, and enter a value in the field beside it. You can click - to remove an option.
   - **Extensible Attributes**: You can add and delete extensible attributes that are associated with a specific DHCP range. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see Managing Permissions.

3. Optionally, you can click Toggle Expert Mode to display the following tabs from which you can modify advanced data.
   - **DDNS**: Complete the following to set DDNS parameters for the range:
     - **Enable DDNS Updates**: Click the check box to enable the Microsoft DHCP server to send dynamic DNS updates or clear the check box to disable this function.
     - **Option 81 Support**: The DHCP server updates DNS only if it is requested by the client. Otherwise, the client updates DNS.
   - **DHCP Server Always Updates DNS**: The DHCP server always updates DNS, regardless of any client request.
   - **Exclusion Ranges**: Configure a range of IP addresses that the server does not use to assign to clients. You can use these exclusion addresses as static IP addresses. For information, see Configuring IPv4 Fixed Addresses. In a split-scope, the exclusion range identifies the range of IP addresses that the other Microsoft server serves. If you edit the exclusion range of either of the scopes in a split-scope and the exclusion ranges no longer complement each other, NIOS removes the split-scope flag from both scopes.
   - **Thresholds**: Thresholds are inherited from the Grid. These watermarks represent thresholds above or below which address usage is unexpected and might warrant your attention.
     - **High-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range exceeds this number, the appliance makes a syslog entry. The default is 95.
     - **Low-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range drops below this number, the appliance makes a syslog entry. The default is 0. Address usage must initially exceed the low-water mark threshold and then dip below it before the appliance considers low address usage an event requiring an alert.

4. Save the configuration and click Restart if it appears at the top of the screen.

or

- Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

Deleting and Restoring a DHCP Range/Scope

When you delete a DHCP range, Grid Manager moves it and its exclusion range and fixed addresses to the Recycle Bin, and permanently deletes its leases. At the next synchronization, the member deletes the scope, its exclusion range and reservations from the Microsoft server. If you restore a DHCP range on Grid Manager, then the Grid member adds its corresponding scope, exclusion range and reservations to the Microsoft server at the next synchronization. For information about deleting DHCP ranges, see Deleting IPv4 Address Ranges. For information about restoring data, see Using the Recycle Bin.

If you delete a scope that is part of a split-scope, Grid Manager automatically removes the split-scope flag from the remaining scope.
Viewing Scopes

To view the scopes in a network, navigate to **DHCP -> Networks -> network**. The panel displays the objects in the network, including the scopes and split-scopes. For split-scopes, the panel displays both scopes with the same start and end address. It displays the following information about each object:

- **IP Address**: The IP address of the DHCP object. For a scope, this field displays the start and end addresses of the scope. Note that the appliance highlights all disabled DHCP objects in gray.
- **Split- Scope**: Displays Yes if the scope is a split-scope.
- **MS Server**: Displays the Microsoft server that is serving the scope.
- **Type**: The DHCP object type, such as DHCP Range or Fixed Address.
- **Name**: The object name. For example, if the IP address belongs to a host record, this field displays the hostname.
- **Comment**: The information you entered for the object.
- **IPv4 DHCP Utilization**: The percentage of the total DHCP usage of a DHCP range. This is the percentage of the total number of fixed addresses, reservations, hosts, and active leases in the DHCP range divided by the total IP addresses in the range, excluding the number of addresses in the exclusion ranges. Note that only enabled objects are included in the calculation.
- **Site**: The site to which the DHCP object belongs. This is one of the predefined extensible attributes.

You can select the following additional columns for display:

- **Static Addresses**: Indicates whether the IP address is a static address.
- **Dynamic Addresses**: Indicates whether the IP address is a dynamically assigned address.
- **Disabled**: Indicates whether the object is disabled.
- **Priority**: Displays the priority of a DHCP range when NAC filters are applied.
- **Available extensible attributes**.

You can also do the following in this panel:

- Sort the displayed data in ascending or descending order by column.
- Click **Go to IPAM View** to view information about the object in the IPAM tab.
- Add new objects, such as DHCP ranges, to the network.
- Delete or schedule the deletion of a selected object or multiple objects.
- Use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see **Using Quick Filters**.
- Print or export the data.

You can also view the scopes in the IP Map.

Adding Fixed Addresses/Microsoft Reservations

To add a reservation from Grid Manager, add a fixed address and Grid Manager synchronizes it to the Microsoft server as a reservation. You can create fixed addresses from scratch or use fixed address templates. For information about fixed address templates, see **Adding IPv4 Fixed Addresses/Reservation Templates**.

To add a fixed address:

1. From the **Data Management** tab, select the **DHCP** tab.
2. Expand the Toolbar and click **Add -> Fixed Address**.
3. In the **Add Fixed Address** wizard, select one of the following and click **Next**:
   - **Add Fixed Address**
   - **Add Fixed Address using Template**
     
5. Click **Next**, and optionally set operational parameters for the fixed address. Otherwise, the fixed address inherits its parameters from its scope.
- **Routers**: In the table, enter the IP address of the router that is connected to the same network as the DHCP client. Click the Add icon to add more routers.
- **Domain Name**: Enter the name of the domain for which the Microsoft DHCP serves DHCP data. The DHCP server includes this domain name in Option 15 when it responds with a DHCPOFFER packet to a DHCPDISCOVER packet from a client.
- **DNS Servers**: In the table, enter the IP address of the DNS server to which the DHCP client sends name resolution requests. The DHCP server includes this information in the DHCPOFFER and DHCPACK messages.
- **Broadcast Address**: Enter the broadcast IP address of the network to which the DHCP server is attached.

6. Click **Next** to enter values for required extensible attributes or add optional extensible attributes. For information, see *Using Extensible Attributes*.

7. Save the configuration and click **Restart** if it appears at the top of the screen.

or

- Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks*.

**Setting Fixed Address/Reservation Properties**

Microsoft reservations inherit their properties from their scopes. In Grid Manager, you can override the inherited values or set other properties of a Microsoft reservation, by editing its fixed address.

To modify a fixed address:

1. From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> **network** -> **fixed_address** check box, and then click the Edit icon.
2. The **Fixed Address** editor contains the following basic tabs from which you can enter data:
   - **General**: You can modify the fields described in 5800935.
   - **IPv4 DHCP Options**: Keep the inherited properties, or override them and enter unique settings. This section displays DHCP and Microsoft vendor options that were synchronized from the Microsoft server. You can edit any of the options. When you select a different User Class or Vendor Class from the drop-down menus, Grid Manager automatically updates the option definitions in the drop-down list.
   - **To configure additional DHCP options, click + and select a User Class and Vendor Class from the drop-down menus. Select an option from the drop-down list, and enter a value in the field beside it. You can click - to remove an option.**
   - **Discovered Data**: If you ran a discovery on the network, Grid Manager displays the discovered data of the fixed address. For information, see *Viewing Discovered Data*. Note that conflicts can occur when discovered data does not match the existing IP address data. For information about resolving these conflicts, see *Resolving Conflicting Addresses*.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with a specific network. You can also modify the values of extensible attributes. For information, see *Using Extensible Attributes*.
   - **Permissions**: This tab appears only if you belong to a superuser admin group. For information, see *Managing Permissions*.

3. Optionally, you can click **Toggle Expert Mode** to display the **DDNS** tab. To set DDNS parameters for the fixed address, complete the following:
   - **Enable DDNS Updates**: Click the check box to enable the Microsoft DHCP server to send dynamic DNS updates or clear the check box to disable this function.
   - **Option 81 Support**
   - **DHCP Server Updates DNS If Requested by Client**: The DHCP server updates DNS only if it is requested by the client. Otherwise, the client updates DNS.
   - **DHCP Server Always Updates DNS**: The DHCP server always updates DNS, regardless of any client request.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

or

- Click the Schedule icon at the top of the wizard to schedule this task. In the *Schedule Change* panel, enter a date, time, and time zone. For information, see *Scheduling Tasks*.

**Deleting and Restoring a Fixed Address/Reservation**

When you delete a fixed address, Grid Manager moves it to the Recycle Bin. At the next synchronization, the Grid member deletes its corresponding reservation from the Microsoft server. If you restore fixed address, then the Grid member adds its corresponding reservation to the Microsoft server at the next synchronization. For information about deleting fixed addresses, see *Deleting Fixed Addresses*. For information about restoring data, see *Using the Recycle Bin*.

**About Superscopes**

In Grid Manager, you can group DHCP ranges served by Microsoft servers into a superscope. You can add multiple DHCP ranges to a superscope, as long as the ranges are all served by the same Microsoft DHCP server. The Grid member then synchronizes the superscope and
its associated DHCP ranges as superscopes and scopes to the Microsoft DHCP server. You can also associate extensible attributes with superscopes in Grid Manager. Extensible attributes are not synchronized to the Microsoft DHCP server. Only admins with read/write permission to superscopes can add and manage superscopes.

Adding Superscopes

Before you add a superscope, you must first create at least one DHCP range to include in the superscope. To add a superscope:

1. From the Data Management tab, select the DHCP tab.
2. If you have more than one network view in the system, select the network view in which you want to add the superscope. The network view must be the same one that is assigned to the Microsoft server.
3. Expand the Toolbar and click Add -> Superscope.
4. In the Add Superscope wizard, complete the following and click Next:
   - Name: Enter a name for the superscope.
   - Comment: Optionally, enter additional information about the superscope.
   - Disabled: Select this to disable the DHCP ranges in the superscope. They are then synchronized as inactive scopes on the Microsoft server.
5. Click the Add icon and select a range from the Select Range dialog box. This dialog box lists only the address ranges that are served by a Microsoft server.
6. Click Next to enter values for required extensible attributes or add optional extensible attributes. For information, see About Extensible Attributes.
7. Save the configuration and click Restart if it appears at the top of the screen.
   or
   - Click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Tasks.

Viewing Superscopes

To view superscopes, navigate to the Data Management tab -> DHCP tab -> Networks tab -> Microsoft Superscopes. Grid Manager displays the following information about each superscope that is displayed:

- **Name**: The name of the superscope. Grid Manager appends the FQDN of its associated Microsoft server so you can identify which superscope belongs to which server.
- **Comment**: The comment that was entered for the superscope.
- **DHCP Utilization**: The percentage of the total DHCP usage of the ranges in the superscope. Fixed addresses and reservations that are outside of a range are excluded from the calculation.
- **Site**: The site of the superscope. This is one of the predefined extensible attributes.

You can add the following columns for viewing:

- **Static Addresses**: The number of static addresses.
- **Dynamic Addresses**: The number of dynamic addresses.
- **Disabled**: Indicates whether the superscope is enabled.

You can do the following in this section:

- Click the link of a superscope to list its address ranges.
- Add a superscope.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Print or export the information in this section.
- Delete a superscope.

Modifying Superscopes

To modify a superscope:

1. From the Data Management tab, select the DHCP tab -> Network tab -> Microsoft Superscopes -> ms_superscope check box, and then click the Edit icon.
2. The Superscopes editor contains the following tabs from which you can modify data:
   - **General**: You can modify the name and comment, and enable or disable the superscope. You can also add and delete address ranges from the superscope. Note that when you delete the last DHCP range in a superscope, Grid Manager automatically deletes the superscope as well.
   - **Extensible Attributes**: Define extensible attributes for the superscope. These apply only when the superscope is managed in Grid Manager. For information, see Using Extensible Attributes.
Permissions: Define administrative permissions that apply to the superscope when it is managed in Grid Manager. For information see About Administrative Permissions.

3. Save the configuration and click Restart if it appears at the top of the screen.

Deleting Superscopes

When you delete a superscope in Grid Manager, it is permanently deleted from the database. The superscope is deleted from the Microsoft server at the next synchronization. Note that deleting a superscope does not delete the DHCP ranges in the superscope. These are retained in the database.

To delete a superscope:

1. From the Data Management tab, select the DHCP tab -> Network tab -> Microsoft Superscopes -> ms_superscope check box, and then click the Delete icon.
2. Click Yes when the confirmation dialog appears.

Synchronizing Updates

A Grid member synchronizes DHCP data with each of its managed Microsoft server at regular intervals. During each synchronization, updates from Grid Manager are applied to the Microsoft server and updates from the Microsoft server are applied to the Grid as well. Because admins can update DHCP data from both the Microsoft server and from Grid Manager, conflicts can occur during synchronization. The following guidelines describe how the Grid member resolves conflicts and handles any differences when DHCP data is synchronized between a Microsoft server and the Grid:

- If a Microsoft server admin modifies an object that has a pending scheduled task in Grid Manager and synchronization occurs before the scheduled task, the object is modified in both the Microsoft server and the Grid member. When the scheduled task executes at its scheduled time, it fails and an error message is logged in the audit log.
- When a Microsoft server admin and a Grid Manager admin change the same object, the Grid member retains the version that exists on the Microsoft server. Following are some examples:

<table>
<thead>
<tr>
<th>Grid Manager Admin...</th>
<th>Microsoft Server Admin...</th>
<th>After Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletes the 10.1.1.0/24 network which has two DHCP ranges</td>
<td>Adds a scope that is within the 10.1.1.0/24 network</td>
<td>The 10.1.1.0/24 network is created on the Grid with the updates and is assigned to the Microsoft server.</td>
</tr>
<tr>
<td>Changes the DHCP options of a scope</td>
<td>Deletes the scope.</td>
<td>The scope is deleted from the Grid as well.</td>
</tr>
</tbody>
</table>

- If a Grid member manages multiple Microsoft servers, it can synchronize scopes to the same network as long as they are served by different Microsoft servers and they do not overlap. If the Microsoft servers have scopes that overlap, the Grid member synchronizes only one of the scopes, including its reservations. It does not synchronize the other scopes and logs an error message for each scope that is not synchronized. For information about the Microsoft logs, see Viewing Synchronization Logs. Note that a Grid member can synchronize scopes with overlapping reservations because they are served by different Microsoft servers.
- When a Grid member synchronizes a split-scope to its respective Microsoft servers, the scopes use the default value for the DHCP Offer Delay value, since this property is not supported by NIOS.
- If you create a split-scope on a NIOS appliance, synchronization fails if there is an existing scope in the same network on one of the Microsoft servers. Only one scope is allowed in a network, per Microsoft server.
- If a Microsoft admin adds a DHCP range and a NIOS admin is in the process of adding the same range when a synchronization occurs, the NIOS admin will not be able to save the range after the synchronization. Grid Manager will display an error message indicating that the range already exists.
- If both a NIOS admin and a Microsoft admin create a scope or split-scope and conflicts occur, the Microsoft server always takes precedence. All conflicts are logged to the Microsoft log. Following are some examples:
  - If the NIOS admin creates a scope and a Microsoft server admin creates a split-scope for the same DHCP range, the split-scope is synchronized to Grid Manager.
  - If the NIOS admin creates a split-scope on Microsoft servers 1 and 2, and a Microsoft admin creates the same split-scope on Microsoft servers 1 and 3 but with different exclusion ranges, the scope created by the NIOS admin on Microsoft server 1 is dropped upon synchronization.
  - If the NIOS admin creates a split-scope on Microsoft servers 1 and 2, and a Microsoft admin creates the same split-scope on the same Microsoft servers but with different exclusion ranges, the split-scope created by the Microsoft admin is synchronized to NIOS and retained. The split-scope created by the NIOS admin is dropped.

Managing Microsoft DHCP Servers

You can control the DHCP services of managed Microsoft servers and set certain properties as well. This section includes the following topics:

- Viewing Members and Managed DHCP Servers
- Setting Microsoft DHCP Server Properties
- Controlling the DHCP Service of a Microsoft Server
- Disabling and Removing Microsoft DHCP Servers
- Modifying DHCP Server Assignments
Viewing Members and Managed DHCP Servers

You can view Infoblox and Microsoft DHCP servers by navigating to the Data Management tab -> DHCP tab, and then selecting the Members/Servers tab. The panel displays the following information about each DHCP server:

- **Name**: The hostname of the Grid member or Microsoft server.
- **Status**: The status of the DHCP service on the Grid member or Microsoft server.
- **Comment**: Comments that were entered for the Grid member or Microsoft server.
- **DHCP Utilization**: The percentage of the total DHCP utilization of the member or Microsoft server. This is the percentage of the total number of DHCP hosts, fixed addresses, reservations, and leases assigned to the member or Microsoft server versus the total number of IP addresses (excluding IP addresses in the exclusion range) and all DHCP objects assigned to the member or DHCP server. Note that only enabled objects are included in the calculation. The appliance updates the utilization data every 15 minutes. The appliance displays the utilization data in one of the following colors:
  - **Red**: The DHCP resources are 100% utilized.
  - **Yellow**: The utilization percentage is over the effective high watermark threshold.
  - **Blue**: The utilization percentage is below the effective low watermark threshold.
  - **Black**: The utilization percentage is at any number other than 100%, or within the effective thresholds.
- **Site**: Values that were entered for this pre-defined attribute.

You can select the following additional columns for display:

- **Address**: The IP address of the member or Microsoft server.
- **Static Addresses**: The number of static IP addresses.
- **Dynamic Addresses**: The number of dynamically assigned IP addresses.

You can do the following:

- Use filters and the Goto function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Goto field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Edit the properties of a Grid member or Microsoft server.
  - Click the check box beside a Grid member or Microsoft server, and then click the Edit icon.
- Export the list of Grid members and Microsoft servers to a .csv file.
  - Click the Export icon.
- Print the list of Grid members and Microsoft servers.
  - Click the Print icon.

Setting Microsoft DHCP Server Properties

From Grid Manager, you can set DHCP properties supported by a Microsoft server. These are applied to the server at the next synchronization. You can also set other properties that apply to Grid Manager only, such as thresholds and the logging.

To set properties for a Microsoft DHCP server:

1. From the Data Management tab, select the DHCP tab -> Members/Servers tab -> Members/Servers -> ms_server check box, and then click the Edit icon.
2. In the Microsoft Server DHCP Properties editor, you can configure DHCP properties in each tab as follows:

   **IPv4 DHCP Options** tab:
   Complete the following to configure basic DHCP options for the server:
   - **Routers**: Click the Add icon and enter the IP address of the router that is connected to the same network as the DHCP clients.
   - **Domain Name**: Enter the name of the domain for which the server serves DHCP data. The DHCP server includes this domain name in Option 15 when it responds with a DHCPOFFER packet to a DHCPDISCOVER packet from a client. If DDNS is enabled on the DHCP server, it combines the host name from the client and this domain name to create the FQDN (fully-qualified domain name) that it uses to update DNS.
   - **DNS Servers**: Click the Add icon and enter the IP address of the DNS server to which the DHCP client sends name resolution requests. The DHCP server includes this information in the DHCPOFFER and DHCPACK messages.
   - **Broadcast Address**: Enter the broadcast IP address of the network to which the DHCP server is attached.
   - **Custom DHCP Options**: This section displays DHCP and Microsoft vendor options that were synchronized from the Microsoft server. You can edit any of the options. When you select a different User Class or Vendor Class from the drop-down menus, Grid Manager automatically updates the option definitions in the drop-down list.
   - To configure additional DHCP options, click + and select a User Class and Vendor Class from the drop-down menus. Select an option from the drop-down list, and enter a value in the field beside it. You can click - to remove an option.

   **DDNS** tab:
   You can enable or disable dynamic DNS updates and set certain properties.
   - **Enable DDNS Updates**: Click the check box to enable the Microsoft DHCP server to send dynamic DNS updates or clear the check box to disable this function.
   - **Option 81 Support**
     - **DHCP Server Updates DNS If Requested by Client**: The DHCP server updates DNS only if it is requested by the client. Otherwise, the client updates DNS.
     - **DHCP Server Always Updates DNS**: The DHCP server always updates DNS, regardless of any client request.
Thresholds tab: Thresholds are inherited from the Grid. These watermarks represent thresholds above or below which address usage is unexpected and might warrant your attention.

- **Enable DHCP Thresholds**: Select this check box to enable the feature.
  - **High-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range exceeds this number, the DHCP server makes a syslog entry. The default is 95.
  - **Low-water Mark**: Enter a number between 0 and 100. If the percentage of allocated addresses in a DHCP range drops below this number, the DHCP server makes a syslog entry. The default is 0. Address usage must initially exceed the low-water mark threshold and then dip below it before the appliance considers low address usage an event requiring an alert.

3. Optionally, you can click **Toggle Expert Mode** to display the **Logging** tab, where you can enable the managing member to log the lease events of the Microsoft server. This setting is inherited from the Grid. You can override that setting by clicking **Override**, and then selecting or clearing the **Log Lease Events from DHCP server** check box.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

**Controlling the DHCP Service of a Microsoft Server**

You can start and stop the DHCP service of a managed Microsoft server from Grid Manager as follows:

1. From the **Data Management** tab, select the **DHCP** tab -> **Members/Servers** tab -> **Members/Servers** -> **ms_server** check box.
2. Expand the Toolbar and click **Start** or **Stop**.
3. Click **Yes** when the confirmation dialog appears.

**Disabling and Removing Microsoft DHCP Servers**

If you remove a Microsoft server as a managed server, Grid Manager deletes all the DHCP ranges, leases, and fixed addresses associated with the server. It also deletes networks that were assigned only to the Microsoft server. It does not delete a network if it was assigned to other Microsoft servers as well.

When you disable a Microsoft server, the managing Grid member terminates any on-going synchronization and restarts synchronization only when the server is re-enabled. The DHCP data associated with that server is preserved in the same state until synchronization resumes.

For information on removing and disabling Microsoft servers, see **Disabling Synchronization** and **Removing a Managed Microsoft Server**.

**Modifying DHCP Server Assignments**

If you disable a Microsoft DHCP server or take it offline for maintenance purposes, for example, you can assign its scopes to a member DHCP server.

Following are the tasks to reassign scopes from a Microsoft server to a member DHCP server:

1. Set the server assignments of all fixed addresses in the scope to "None".
   - From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> network -> fixed_address check box, and then click the **Edit** icon. You can change the server assignment in the **General** tab of the **Fixed Address** editor.
2. Set the server assignments of all address ranges served by the Microsoft server to "None".
   - From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> network -> addr_range check box, and then click the **Edit** icon. You can change the server assignment in the **General** tab of the **DHCP Range** editor.
3. Change the server assignments of the networks by deleting the Microsoft server and replacing it with a member DHCP server.
   - From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> network check box, and then click the **Edit** icon. You can change the server assignment in the **Member Assignment** tab of the **Network** editor. contains the following basic tabs from which you can modify data:
4. Modify the server assignments of all address ranges and specify the member DHCP server.
   - From the **Data Management** tab, select the **DHCP** tab -> **Networks** tab -> **Networks** -> network -> addr_range check box, and then click the **Edit** icon. You can change the server assignment in the **General** tab of the **DHCP Range** editor.
5. Restart services.

The member DHCP server starts granting lease requests after the restart. Note that you do not need to clear the leases that were active on the Microsoft server, because the member automatically clears them when you change the DHCP server assignment.

**Part 7 Monitoring and Reporting**

This section explains how to use the different monitoring and reporting tools, including DHCP fingerprint detection and SNMP. It includes the following chapters:

- **Chapter 37, Monitoring the Appliance**
- **Chapter 38, DHCP Fingerprint Detection**
- **Chapter 39, Monitoring with SNMP**
- **Chapter 40, Infoblox Reporting and Analytics**
- **Chapter 41, Infoblox Reporting Model**
Chapter 37 Monitoring the Appliance

This chapter describes the status icons that indicate the state of appliances, services, database capacity, Ethernet ports, HA, and Grid replication. It also explains how to use the various logs and the traffic capture tool to monitor a NIOS appliance.

This chapter contains the following sections:

- Viewing Status
  - Grid Status
  - Member Status
  - Viewing the Grid Node Tree
  - Enabling Grid Visualization
- Monitoring Services
  - Service Status
  - Monitoring Grid Services
  - Monitoring Member Services
- Using a Syslog Server
  - Specifying Syslog Servers
  - Configuring Syslog Backup Servers
  - Configuring Syslog for Grid Members
  - Setting DNS Logging Categories
  - Viewing the Syslog
  - Viewing the RPZ Threat Details
  - Searching in the Syslog
  - Downloading the Syslog File
- Capturing DNS Queries and Responses
  - Capturing DNS Queries
  - Capturing DNS Responses
  - Configuring DNS Query and Response Captures
  - Excluding Domains From Query and Response Capture
- Monitoring Tools
  - Using the Audit Log
  - Viewing the Replication Status
  - Using the Traffic Capture Tool
  - Using the Capacity Report
  - Participating in the Customer Experience Improvement Program
  - Monitoring DNS Transactions
  - Viewing DNS Alert Indicator Status
  - Configuring DNS Alert Thresholds
- Tracking Object Changes in the Database
  - Best Practices for Object Change Tracking
  - Enabling Object Change Tracking
  - Using Full Synchronization
  - Using Incremental Synchronization

Viewing Status

Grid Manager provides tools for monitoring the status of the Grid, members, and services. You can monitor overall Grid and member status from the Dashboard, which provides a high-level view of your Grid, members and IP address data, and easy access to tasks. For information, see Dashboards.

Grid Manager also displays status icons to indicate the state of appliances, services, database capacity, Ethernet ports, HA, and Grid replication. Depending on your appliance, Grid Manager can display status icons for the power supplies as well as icons to indicate the state of the RAID array and disk controller backup battery.

You can monitor detailed status of the Grid, members, and services, and then decide how to manage them. Note that when any member or service encounters issues, the appliance sends SNMP traps. For information, see Monitoring with SNMP.

Capturing DNS Queries and Responses

You can capture DNS queries and responses for later analysis. When configuring this feature, you can choose to save the capture file locally on your appliance, as well as on the FTP (File Transfer Protocol) or SCP (Secure Copy) server. When you save it locally, you can use show capture to view the contents of the capture file. You can also use filter commands to exclude certain queries and view only the desired ones. Note that using multiple CLI commands to filter data for the appliances with large number of captured DNS queries and responses can significantly affect the system performance, protocol performance, and CLI command performance. For more information about CLI commands, refer to the Infoblox CLI Guide.

Note: The DNS queries and responses captured on an IB-4030 appliance does not contain cached query information.
A capture file for logging DNS queries and responses is rolled over based on the configured time limit or when the file reaches 100 MB in size, whichever is sooner. The default time limit is 10 minutes. The capture file is automatically saved and exported to an FTP or SCP server based on your configuration. When you configure the appliance to save the capture file locally and later enable FTP or SCP, the appliance copies all the data starting with the oldest data. Infoblox recommends that you constantly monitor the FTP or SCP server to ensure that it has sufficient disk space. DNS queries and responses are stored on the appliance if the FTP or SCP server becomes unreachable. The maximum storage capacity varies based on the appliance model. After reaching the maximum limit, the appliance overwrites the old data with the new one. For information about the maximum hard drive space, see Maximum Hard Drive Space used for DNS queries and Responses. The amount of data captured depends on the DNS query rate and the domains that are included in or excluded from the capture. For information about how to exclude domains, see Excluding Domains From Query and Response Capture.

Capturing DNS Queries

You can capture queries to all domains or limit the capture to specific domains. You can also apply the Bulk Add Domains feature to tailor query capture to a desired subset of domains or zones. When capturing DNS queries, NIOS matches the specified domain name(s) and everything that belongs to the domain. For example, when you specify 'foo.com' as the domain, NIOS captures queries sent to 'foo.com,' 'mail.foo.com,' and 'ftp.foo.com.' NIOS captures queries to domains for which a name server is authoritative; it also captures recursive queries. Note that this feature does not support wildcard characters or regular expressions.

DNS Query Message Format

The DNS query generates a query message in the following format:

```
<dd-mmm-yyyy HH:MM:SS.uuu> <client ip>#<port> query: <query_Domain name> <class name> <type name> <- or +>[SETDC] <(name server ip)>
```

where

+ = recursion
- = no recursion
S = TSIG
E = EDNS option set
T = TCP query
D = EDNS 'DO' flag set
C = 'CD' message flag set

Following is a sample DNS query message:

```
30-Apr-2013 13:35:02.187 client 10.120.20.32#42386: query: foo.com IN A + (100.90.80.102)
```
+ = recursion available (from DNS message header)
A = authoritative answer (from DNS message header)
t = truncated response (from DNS message header)
E = EDNS OPT record present (from DNS message header)
D = DNSSEC OK (from EDNS OPT RR)
V = responding server has validated DNSSEC records
L = response contains DTC synthetic record

Following are some DNS response samples:

Example 1: When querying an A record
07-Apr-2013 20:16:49.083 client 10.120.20.198#57398 UDP: query: a2.foo.com IN A response: NOERROR +AED
a2.foo.com. 28800 IN A 1.1.1.2;

Example 2: When querying an AAAA record
07-Apr-2013 20:16:49.083 client 10.120.20.198#57398 UDP: query: a4.foo.com IN AAAA response: NOERROR +AED
a4.foo.com. 28800 IN AAAA ab::a;

Example 3: When querying an A record over IPv6
a2.foo.com. 28800 IN A 1.1.1.2;

Example 4: When querying an A record over TCP
07-Apr-2013 20:16:49.083 client 10.120.20.198#57398 TCP: query: a2.foo.com IN A response: NOERROR +ED
a2.foo.com. 28800 IN A 1.1.1.2;

Example 5: When querying ANY record
07-Apr-2013 20:16:49.083 client 10.120.20.198#57398 UDP: query: a2.foo.com IN ANY response: NOERROR +ED
a2.foo.com. 28800 IN A 1.1.1.2;

Example 6: When querying an A record with multiple addresses
07-Apr-2013 20:16:49.083 client 10.120.20.198#57398 UDP: query: a1.foo.com IN A response: NOERROR +ED
a1.foo.com. 28800 IN A 1.1.1.1; a1.foo.com. 28800 IN A 11.1.1.1;

Example 7: When querying an aliased A record
07-Apr-2013 20:16:49.083 client 10.120.20.198#57398 UDP: query: c2.foo.com IN A response: NOERROR +ED
c2.foo.com. 28800 IN CNAME a2.foo.com.; a2.foo.com. 28800 IN A 1.1.1.2;

Example 8: When querying an NXDOMAIN
07-Apr-2013 20:16:49.083 client 10.120.20.198#57398 UDP: query: non-exist.foo.com IN A response: NXDOMAIN +ED

Example 9: Response message for NOERROR/nodata
07-Apr-2013 20:16:49.083 client 10.120.20.198#57398 UDP: query: a1.foo.com IN SRV response: NOERROR +ED

Example 10: Response message for refused query
07-Apr-2013 20:16:49.083 client 10.120.20.198#57398 UDP: query: refused.com IN A response: REFUSED +ED

Example 11: Response message when server fails
07-Apr-2013 20:16:49.083 client 10.120.20.198#57398 UDP: query: servfail.com IN A response: SERVFAIL +E

Example 12: Response message when query A record in a signed zone
07-Apr-2013 20:16:49.083 client 10.120.20.198#57398 UDP: query: a1.signed.com IN A response: NOERROR +ED
a1.signed.com. 28800 IN A 1.1.1.1;

Example 13: Response message for explicit query to DNSSEC RRs
07-Apr-2013 20:16:49.083 client 10.120.20.198#57398 UDP: query: a1.signed.com IN RRSIG response: NOERROR +ED
a1.signed.com. 28800 IN RRSIG A 5 3 28800 20130616004903 20130611234903 4521 signed.com. eVROKe7RbnkJFTaumTJ3JJG76bduFLfdeEEnszitXHqCbnYy5zDy+qbUIHCQuN/1dCnT7bZEBEMzuatzfms+2Y5ZKZsU67P9Yg6GkOMwsf2LcJ1Bm/
Configuring DNS Query and Response Captures

To configure DNS query and response captures:

1. **Grid**: From the **Data Management** tab, select the **DNS** tab, expand the **Toolbar** and click **Grid DNS Properties**.
   - **Member**: From the **Data Management** tab, select the **DNS** tab and click the **Members** tab -> **member** check box -> **Edit** icon.

2. In the **Grid DNS Properties** or **Member DNS Properties** editor, click **Toggle Advanced Mode** and select the **Logging** tab.

3. Under **Data Collection for all DNS Queries/Responses to a Domain**, complete the following:
   - Select the **Capture DNS Queries** check box to start capturing DNS queries. This enables the feature set for configuration. When you enable this option at the member level, the appliance captures DNS queries for the selected members only.
   - Select the **Capture DNS Responses** check box to start capturing DNS responses. This enables the feature set for configuration. When you enable this option at the member level, the appliance captures DNS responses for the selected members only.

   **Note**: Enabling the logging of queries and responses at the same time can increase disk space usage and adversely affect DNS services and performance. Infoblox recommends that you do not configure both logging at the same time.

   - Select **Capture queries/responses for all domains** to capture queries and responses to all domains and zones.
   - Select **Limit capture to these domains** to capture DNS queries and responses to domains and zones one at a time.
   - Specify domains for DNS capture operations in the Domain table by clicking the **Add** icon, and choosing **Add Domain** or **Bulk Add Domains** from the menu.
   - To define the destination for capture files, do the following:
     - **Retain captured queries on the local disk**: Select this check box to save the DNS queries on the appliance. In addition to the local disk, you can select to export the DNS queries to the remote server by selecting SCP in the Export to drop-down list.
     - **Export to**: From the drop-down list, select SCP to back up the DNS queries on the remote server and **None** to save queries only on the appliance. To save the captured DNS queries on both the appliance and the remote server, select the **Retain captured queries on the local disk** check box and SCP from the Export to drop-down list.

   **Note**: When you configure an SCP server and enable the MGMT port, the NIOS appliance uses SSH for data transfer. It uses the same authentication and provides the same security as SSH. SCP uses the LAN1 port to communicate with the external servers.

   - When you select FTP or SCP from the Export to drop-down list, complete the following:
     - In the Directory Path field, enter the directory to which the capture file will be saved on the server. Infoblox recommends that you use the ~ symbol for the remote server.
     - In the Server Address field, enter the IP address of the remote server to which the capture files will be saved.
     - Enter the file server account **Username** and **Password** values.
     - **Limit query data collected per file to minutes or 100MB (whichever comes first)**: This option limits the collection of query data per capture file. A capture file for logging DNS queries and responses is rolled over based on the configured time limit or when the file reaches 100 MB in size, whichever is sooner. The default time limit is 10 minutes. You can enter a value from 1 to 10.

   4. Save the configuration.

   **Table 37.2** lists the maximum hard drive space required for capturing DNS queries and responses for supported Infoblox appliance models.

**Table 37.2 Maximum Hard Drive Space used for DNS queries and Responses**

<table>
<thead>
<tr>
<th>Supported Infoblox Appliances</th>
<th>Maximum Hard Drive Space for DNS Query /Response Capture (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trinzic 100</td>
<td>400</td>
</tr>
<tr>
<td>Trinzic 810</td>
<td>900</td>
</tr>
<tr>
<td>Trinzic 815 and IB-V815</td>
<td>900</td>
</tr>
<tr>
<td>Trinzic 820</td>
<td>3100</td>
</tr>
<tr>
<td>Trinzic 825 and IB-V825</td>
<td>3100</td>
</tr>
<tr>
<td>Trinzic 1410</td>
<td>6000</td>
</tr>
<tr>
<td>Trinzic 1415 and IB-V1415</td>
<td>6000</td>
</tr>
<tr>
<td>Model</td>
<td>Price</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Trinzic 1420</td>
<td>10000</td>
</tr>
<tr>
<td>Trinzic 1425 and IB-V1425</td>
<td>10000</td>
</tr>
<tr>
<td>Trinzic 2210</td>
<td>12000</td>
</tr>
<tr>
<td>Trinzic 2215 and IB-V2215</td>
<td>12000</td>
</tr>
<tr>
<td>Trinzic 2220</td>
<td>28000</td>
</tr>
<tr>
<td>Trinzic 2225 and IB-V2225</td>
<td>28000</td>
</tr>
<tr>
<td>Infoblox-4010</td>
<td>40000</td>
</tr>
<tr>
<td>IB-VM-100</td>
<td>400</td>
</tr>
<tr>
<td>IB-VM-2000 (120G)</td>
<td>15000</td>
</tr>
<tr>
<td>IB-VM-810 (120G)</td>
<td>900</td>
</tr>
<tr>
<td>IB-VM-820</td>
<td>3100</td>
</tr>
<tr>
<td>IB-VM-1410 (120G)</td>
<td>6000</td>
</tr>
<tr>
<td>IB-VM-1420 (120G)</td>
<td>10000</td>
</tr>
<tr>
<td>IB-VM-2210 (120G)</td>
<td>12000</td>
</tr>
<tr>
<td>IB-VM-2220 (120G)</td>
<td>28000</td>
</tr>
<tr>
<td>IB-VM-4010 (120G)</td>
<td>40000</td>
</tr>
<tr>
<td>PT-1400</td>
<td>10000</td>
</tr>
<tr>
<td>PT-1405</td>
<td>10000</td>
</tr>
<tr>
<td>PT-2200</td>
<td>28000</td>
</tr>
<tr>
<td>PT-2205</td>
<td>28000</td>
</tr>
<tr>
<td>PT-4000</td>
<td>40000</td>
</tr>
</tbody>
</table>

Excluding Domains From Query and Response Capture

You can exclude individual domains and their subdomains from DNS query and response capturing. You can also use the Bulk Add Domains feature for a subset of domains to exclude them from query and response capturing. Subdomains can also be specified for exclusion. NIOS matches the specified domain names and their subdomains while filtering them in the Exclusion list. For example, when you specify 'foo.com' as the domain to be excluded, NIOS filters queries for 'foo.com,' 'mail.foo.com,' and 'ftp.foo.com.'

**Note:** IDNs are not supported for the domains that are added to the Inclusion list and Exclusion list. You can use the punycode representation of an IDN in these lists.

To exclude a domain from query and response capturing, do the following:

1. **Grid:** From the **Data Management** tab, select the **DNS** tab, expand the **Toolbar** and click **Grid DNS Properties.**
2. **Member:** From the **Data Management** tab, select the **DNS** tab and click the **Members** tab -> member check box -> Edit icon.
3. **In the Grid DNS Properties or Member DNS Properties editor,** click **Toggle Advanced Mode** and select the **Logging** tab.
4. **Under Data Collection for all DNS Queries/Responses to a Domain,** select the **Exclude the following domains** check box.

**Note:** NIOS first matches the domains in the Exclusion list and then matches the domains in the Inclusion list. NIOS does not capture queries and responses for the subdomains in the **Capture DNS Queries/Responses** list (Inclusion list) if their domains are added to the **Exclude the following domains list** (Exclusion list).

The following table provides examples of domains and subdomains added to the Inclusion and Exclusion lists and the corresponding effects on the query and response capture operations:
<table>
<thead>
<tr>
<th>Capture DNS Queries/Responses (Inclusion List)</th>
<th>Exclude the following domains (Exclusion List)</th>
<th>Queried Domain</th>
<th>Queries/Responses Captured</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>foo.com</td>
<td>--</td>
<td>• foo.com • finance.foo.com</td>
<td>Yes</td>
<td>Exclusion list is empty and therefore matches the Inclusion list. NIOS captures queries/responses made to foo.com and finance.foo.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• corp1.com</td>
<td>No</td>
<td>NIOS does not capture queries/responses made to corp1.com as this domain is not mentioned in the Inclusion list.</td>
</tr>
<tr>
<td>Capture All</td>
<td>foo.com</td>
<td>• foo.com</td>
<td>No</td>
<td>Matches the Exclusion list and NIOS does not capture queries made to foo.com.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• finance.foo.com</td>
<td>No</td>
<td>Subdomain matches the Exclusion list and NIOS does not capture queries/responses made to finance.foo.com.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• corp1.com</td>
<td>Yes</td>
<td>Does not match the Exclusion list. Matches the Inclusion list and therefore NIOS captures queries/responses made to corp1.com.</td>
</tr>
<tr>
<td>foo.com</td>
<td>it.foo.com</td>
<td>• foo.com • finance.foo.com</td>
<td>Yes</td>
<td>Does not match the Exclusion list and therefore NIOS captures queries/responses made to foo.com and finance.foo.com.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• it.foo.com • ms.it.foo.com</td>
<td>No</td>
<td>Matches the Exclusion list and excludes their subdomains. NIOS does not capture queries/responses made to it.foo.com and ms.it.foo.com.</td>
</tr>
<tr>
<td>it.foo.com</td>
<td>foo.com</td>
<td></td>
<td></td>
<td>Domain is added to the Exclusion list and its subdomain is added to the Inclusion list. Therefore, this is not a valid configuration as queries/responses are not captured. The appliance displays a warning message for such invalid configuration.</td>
</tr>
<tr>
<td>it.foo.com</td>
<td>it.foo.com</td>
<td></td>
<td></td>
<td>Domain is added to both the Exclusion and Inclusion lists. This is not a valid configuration as queries/responses are not captured. The appliance displays a warning message for such invalid configuration.</td>
</tr>
</tbody>
</table>
Enabling Grid Visualization

To enable Grid visualization:

1. From the Grid tab, select the Grid Manager tab -> Members tab, and then click Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, click the Advanced tab.
3. Select the Show Grid Visualization check box.
4. Click Save to save the changes. The Visualization tab appears and displays a graphical representation of the Grid. This may take a long time depending on the number of members you have in the Grid. When you deselect this check box, you disable Grid visualization for all users.

Grid Status

You can monitor the overall status of the Grid using the Grid Status widget on the Dashboard. For information, see Grid Status.

You can also view the Grid status from the Grid Manager tab. To view Grid status, from the Grid tab, select the Grid Manager tab. Grid Manager displays the overall Grid status and status of all Grid services. The Grid status represents the status of the most critical members or services in the Grid. When all Grid members are running properly, the overall Grid status is green. When one of the members has operational problems, the overall Grid status is red. Grid Manager lists all Grid members in the Members tab so you can identify which member has issues. For information, see Member Status.

In addition, the service bar below the Grid status lists the status of all licensed services on your Grid. This can include DHCP, DNS, Cloud-API, TFTP, HTTP (File Distribution), FTP, NTP, bloxTools, Captive Portal, DNS Accelerator, Reporting, Discovery and others, depending on the active licenses you have installed. When you click a service link, Grid Manager displays detailed information about the selected service running on all members. For information, see Monitoring Services. Grid Manager also provides icons you can use to edit Grid properties and bookmark the page.

Member Status

You can monitor the overall status, such as the memory usage and system temperature, of a Grid member or an independent appliance using the Member Status (System Status) widget on the Dashboard. For information, see Member Status (System Status).

To monitor detailed status of a member, from the Grid tab, select the Grid Manager tab -> Members tab.

In the Members tab, Grid Manager displays the Grid Master first and then all other members in alphabetical order. If a member is an HA pair, you can click the arrow next to the member row to view information about the active and passive nodes. Grid Manager can display the following information:

- **Name**: The name of the member.
- **HA**: Indicates whether the member is an HA pair.
- **Status**: The service status of the member. For a vNIOS appliance whose license is revoked and is still operating in the Grid, Grid Manager displays a license violation warning here. You should immediately remove this member from the Grid.
- **IPv4 Address**: The IPv4 address of the appliance, or the VIP of an HA pair.
- **IPv6 Address**: The IPv6 address of the appliance, or the VIP of an HA pair.
- **Identify**: This field appears only if your appliance has the unit identification button. When you identify the appliance by pressing the UID button on the appliance or through the GUI or CLI command, this field displays On. Otherwise, this is Off.
- **DHCP, DNS, TFTP, HTTP, FTP, NTP, bloxTools, Captive Portal, DNS Accelerator usage, Reporting, Discovery, Threat Protection, Cloud-API, Threat Analytics, TAXII**: The status icons indicate whether these services are running properly. The DNS accelerator usage feature is only applicable to the IB-4030 appliance. For information, see Service Status.
- **Hardware Type**: The hardware type of the appliance.
- **Hardware Model**: The hardware model of the appliance.
- **Serial Number**: The serial number of the appliance.
- **DB Utilization**: The current percentage of the database in use.
- **Platform**: The platform on which the appliance is running. For vNIOS virtual appliances, this displays the name of the CMP, such as AW, S, Azure, or VMware. For physical NIOS appliances, this displays Physical.
- **Comment**: Information about the member.

To turn the identification button on or off on the member, click the Hardware Identify icon from the horizontal navigation bar. Grid Manager displays a panel with the appliance name, status, and IP address. Hover your mouse over the row and click Turn On to turn the identification button on, or click Turn Off to turn it off.

To view detailed status, select a member check box, and then click the Detailed Status icon. Grid Manager displays the Detailed Status panel. If
the selected member is an HA pair, Grid Manager displays the information in two columns, one for the active node and the other for the passive. The Detailed Status panel provides detailed information described in the following sections.

You can modify some of the data in the table. Double click a row, and either modify the data in the field or select an item from a drop-down list. Click Save to save the changes. Note that some fields are read only.

Appliance Status

The status icon indicates the operational status of a Grid member and a general description of its current operation. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The appliance is operating normally in a “Running” state.</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>The appliance is connecting or synchronizing with its Grid Master.</td>
<td></td>
</tr>
<tr>
<td>Red</td>
<td>The Grid member is offline, is not licensed (that is, it does not have a DNSone license with the Grid upgrade that permits Grid membership), is upgrading or downgrading, or is shutting down.</td>
<td></td>
</tr>
</tbody>
</table>

The following are descriptions that may appear: Running, Offline, Error, and Warning.

Disk Usage

Grid Manager displays the percentage of the data partition of the hard disk drive that is currently in use on the selected Grid member. It also displays whether the percentage of usage has exceeded the trigger or reset value. Note that the trigger and reset values are user configurable. The default trigger value is 85% and reset value is 70%. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The disk usage is either below the reset value or has not yet reached the trigger value.</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>The disk usage is decreasing from the trigger value, but has not yet reached the reset value.</td>
<td></td>
</tr>
<tr>
<td>Red</td>
<td>The disk usage has exceeded the trigger value.</td>
<td></td>
</tr>
</tbody>
</table>

DB Capacity Usage

Grid Manager displays the current percentage of the database in use on the selected Grid member. It also describes whether the usage has exceeded the trigger or reset value. Note that the trigger and reset values are user configurable. The default trigger value is 80% and reset value is 70%. For information, see Using the Capacity Report. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The database capacity is either below the reset value or has not yet reached the trigger value.</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>The database capacity is decreasing from the trigger value, but has not yet reached the reset value. When the capacity exceeds the trigger value, the icon changes from green to yellow.</td>
<td></td>
</tr>
</tbody>
</table>

LAN1/LAN2 Ports, HA Port, and MGMT Port

Grid Manager displays the IP address of the port. The status icons for these ports indicate the state of their network connectivity.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The port is properly connected to a network. Grid Manager displays the IP address of the network.</td>
<td></td>
</tr>
<tr>
<td>Red</td>
<td>The port is not able to make a network connection.</td>
<td></td>
</tr>
<tr>
<td>Gray</td>
<td>The port is disabled.</td>
<td></td>
</tr>
</tbody>
</table>
The LCD status icon indicates its operational status.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>The LCD is functioning properly.</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>The LCD process is not running.</td>
</tr>
</tbody>
</table>

Memory Usage

Grid Manager displays the current percentage of system memory in use on the selected Grid member. It also describes whether the usage has exceeded the trigger or reset value. Note that the trigger and reset values are user configurable. The default trigger value is 90% and reset value is 80%. You can see more details about memory usage through the CLI command: show memory. The status icon can be one of the following.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Red</td>
<td>The memory usage has exceeded the trigger value.</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>The memory usage is decreasing from the trigger value, but has not yet reached the reset value.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>The memory usage is either below the reset value or has not yet reached the trigger value.</td>
</tr>
</tbody>
</table>

Swap Usage

Grid Manager displays the current percentage of swap area in use on the selected Grid member. It also describes whether the usage has exceeded the trigger or reset value. Note that the trigger and reset values are user configurable. The default trigger value is 20% and reset value is 10%. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Red</td>
<td>The memory usage has exceeded the trigger value.</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>The memory usage is decreasing from the trigger value, but has not yet reached the reset value.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>The memory usage is either below the reset value or has not yet reached the trigger value.</td>
</tr>
</tbody>
</table>

FAN

The status icon indicates whether the fan is functioning properly. The corresponding description displays the fan speed. The status icon and fan speed are displayed for Fan1, Fan2, and Fan3.

**Note:** vNIOS appliances on VMware do not monitor or report the fan speed.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>The fan is functioning properly.</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>The fan is not running.</td>
</tr>
</tbody>
</table>

Power Supply

The Infoblox-4010 has redundant power supplies. The power supply icon indicates the operational status of the power supplies.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>The power supplies are functioning properly.</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>One power supply is not running. To find out which power supply failed, check the LEDs of the power supplies.</td>
</tr>
</tbody>
</table>

NTP Synchronization
The status icon indicates the operational status of the current NTP synchronization status.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>The NTP service is enabled and running properly.</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>The NTP service is enabled, and the appliance is synchronizing its time.</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>The NTP service is enabled, but it is not running properly or is out of synchronization.</td>
</tr>
<tr>
<td></td>
<td>Gray</td>
<td>The NTP service is disabled.</td>
</tr>
</tbody>
</table>

**Passive HA Connectivity Status**

The status icon indicates the ARP connectivity status of the passive node of an HA pair. The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>The passive HA node is connected to the local router.</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>The passive HA node fails to connect to the local router.</td>
</tr>
<tr>
<td></td>
<td>Gray</td>
<td>ARP is disabled on the passive node of an HA pair.</td>
</tr>
</tbody>
</table>

**CPU Temperature**

This icon is always green. The description reports the CPU temperature.

*Note: vNIOS appliances on VMware do not monitor or report the CPU temperature.*

**System Temperature**

This icon is always green. The description reports the system temperature.

*Note: vNIOS appliances on VMware do not monitor or report the system temperature.*

**CPU Usage**

Grid Manager displays the current percentage of the CPU usage on the selected Grid member. The maximum is 100%. It also describes whether the CPU usage has exceeded the trigger or reset value. Note that the trigger and reset values are user configurable. The default trigger value is 81% and reset value is 70%. You can see more details about CPU usage through the CLI command: show CPU.

The status icon can be one of the following:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>The CPU usage is either below the reset value or has not yet reached the trigger value.</td>
</tr>
<tr>
<td></td>
<td>Red</td>
<td>The CPU usage has exceeded the trigger value.</td>
</tr>
</tbody>
</table>

**RAID**

For the Infoblox-4010, Grid Manager displays one of the following icons to indicate the status of each disk in the RAID array. Next to the status icon is a summary that includes the disk number, the operational status of the disk, and the disk type. Grid Manager also displays a RAID summary with an overall array status icon and the percentage at which the array is currently operating.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>The RAID array or the disk is functioning properly.</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>A new disk has been inserted and the RAID array is rebuilding.</td>
</tr>
</tbody>
</table>
The RAID array or the disk is degraded. At least one disk in the array is not functioning properly. Grid Manager lists the disks that are online. Replace only the disks that are offline.

In the event of a disk failure, you must replace the failed disk with one that is qualified and shipped from Infoblox and has the same disk type as the rest of the disks in the array. The appliance displays information about mismatched disks. Infoblox-4010 uses only the IB-Type 3 disk type. All disk drives in the array must have the same disk type for the array to function properly. You can have either IB-Type 1, IB-Type 2, or IB-Type 3, but you cannot mix both in the array. When you have a mismatched disk in the array, you must promptly replace the disk with a replacement disk from Infoblox to avoid operational issues.

**RAID Battery**

The icon indicates the status of the disk controller backup battery on the Infoblox-4010.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The battery is charged. The description indicates the estimated number of hours of charge remaining on the battery.</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>The battery is charging.</td>
<td></td>
</tr>
<tr>
<td>Red</td>
<td>The battery is not charged.</td>
<td></td>
</tr>
</tbody>
</table>

**Monitoring Services**

The Grid or device status icon and the service icon indicates whether a service running on a member or an independent appliance is functioning properly or not.

**Service Status**

After you enable any of the services — DHCP, DNS, TFTP, HTTP (for file distribution), FTP, NTP, bloxTools, Captive Portal, Reporting, Discovery, Threat Protection and Cloud API — the appliance indicates their status as follows:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The service is enabled and running properly.</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>The service is enabled, but there may be some issues that require attention. For Threat Protection, this could mean that one of the members is in monitor mode.</td>
<td></td>
</tr>
<tr>
<td>Red</td>
<td>The service is enabled, but it is not running properly. (A red status icon can also appear temporarily when a service is enabled and begins running, but the monitoring mechanism has not yet notified Grid Manager.)</td>
<td></td>
</tr>
<tr>
<td>Gray</td>
<td>The service is not configured or it is disabled.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** When you enable reporting service on the Grid and configure multi-site cluster, you can monitor the status of all reporting members that you have configured. For information about reporting clusters, see Configuring Reporting Clusters.

**Monitoring Grid Services**

The status icon of a Grid service represents the status of the most critical service in the Grid. For example, if the Grid DHCP status icon is red, the DHCP service on one of the members in the Grid is not running properly. You can click the DHCP service link to view the service status of all Grid members and identify which member has a service problem. You can then decide to start or stop the service, or modify the service configuration on that member.

To monitor a Grid service:

1. From the Grid tab, select the Grid Manager tab, and then click a service link.
2. Grid Manager displays the following information in the Services tab:
   - **Name**: The name of the member.
   - **Service Status**: The current status of the service.
   - **IPv4 Address**: The IPv4 address of the appliance or the VIP of an HA pair.
   - **IPv6 Address**: The IPv6 address of the appliance or the VIP of an HA pair.
   - **Comments**: Information about the member or service.
   - **Site**: The site to which the member belongs. This is one of the predefined extensible attributes. You can select available extensible attributes for display.
   - **Reporting Site**: This field appears only when you enable the reporting service and configure the multi-site cluster. For
information about how to configure the multi-site clustering mode, see Configuring Reporting Clusters.

Note: The Reporting Site column is hidden by default. To display this column, click the down arrow next to any column header and select Columns -> Edit Columns -> Reporting Site check box and click Apply. If the Reporting Site column is visible, then the extensible attribute value is automatically updated.

3. Optionally, click the Edit icon next to the service name to edit the Grid properties for the service.

or

Select a member check box, and do one of the following:

- Click the Edit icon to edit the member service configuration. Grid Manager displays the editor for the corresponding service. For example, when you edit the DHCP service, Grid Manager displays the Member DHCP Configuration editor.
- Click the Start icon to start the service.
- Click the Stop icon to stop the service.

Grid Manager updates the service status based on your action.

Monitoring Member Services

You can view detailed service status on a selected member. Optionally, you can start and stop a service, and edit the service configuration.

To monitor a member service:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> member check box, and then click the Manage Member Services icon.

In the Manage Services panel, Grid Manager displays the following information:

- **Service**: The name of the service.
- **Status**: The current status of the service running on the member.
- **Description**: The description of the status. Grid Manager displays the percentage of usage for the TFTP, HTTP (File Distribution), FTP, and bloxTools services.

2. Optionally, mouse over a service and do one of the following:

   - **Start/Stop Service**: Click this icon to start or stop the selected service. For example, when the DNS service is currently stopped, the appliance starts the service when you click this icon.
   - **Edit Service**: Click this icon to edit the selected service. Grid Manager displays the corresponding editor. For example, when you click the Edit Service icon for DNS, Grid Manager displays the Member DNS Configuration editor.

3. Click the Refresh icon to update the service status.

Monitoring Tools

You can use the audit log, the replication status, the traffic capture tool, and the capacity report in a Grid or HA pair to monitor administrative activities and capture traffic for diagnostic purposes. You can also use CLI commands to monitor certain DNS transactions.

This section includes the following topics:

- Using the Audit Log
- Viewing the Replication Status
- Using the Traffic Capture Tool
- Using the Capacity Report
- Participating in the Customer Experience Improvement Program
- Monitoring DNS Transactions
- Viewing DNS Alert Indicator Status
- Configuring DNS Alert Thresholds

In addition, if Grid members manage Microsoft servers, Grid Manager creates a synchronization log file for each managed Microsoft server. For information, see Viewing Synchronization Logs.

Using the Audit Log

The audit log contains a record of all Infoblox administrative activities. It provides the following detailed information:

- Timestamp of the change. If you have different admin accounts with different time zone settings, the appliance uses the time zone of the admin account that you use to log in to the appliance to display the date and timestamp.
- Administrator name
- Changed object name
- New value of the object. If you change multiple properties of an object, the audit log lists all changes in a comma-separated log entry.

You can also search the audit log to find the new value of an object.
The appliance logs the following successful operations:

- Logins to Grid Manager and the API.
- Logout events, including when users log out by clicking the Logout button, when the Grid Manager GUI times out, and when users are logged out due to an error.
- Write operations such as the addition, modification, and deletion of objects.
- System management operations such as service restarts and appliance reboots.
- Scheduled tasks such as adding an A record or modifying a fixed address.

### Enabling Audit Log Rolling

When the audit log reaches its maximum size, which is 100 MB, the appliance automatically writes the file into a new file by adding a .0 extension to the first file and incrementing subsequent file extensions by 1. Files are compressed during the rotation process, adding a .gz extension following the numerical increment. The sequential incrementation goes from zero through nine. When the eleventh file is started, the tenth log file (file.9.gz) is deleted, and subsequent files are renumbered accordingly. For example, the current log file moves to file.0.gz, the previous file.0.gz moves to file.1.gz, and so on through file.9.gz. A maximum of 10 log files (0-9) are kept. To list the audit log files and their sizes, log in to the Infoblox CLI and execute the show logfiles command.

To enable audit log rolling:

1. From the Grid tab, select the Grid Manager tab -> Members tab, and then click Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the Security tab, and then select Enable Audit Log Rolling.

### Specifying the Audit Log Type

Select either the Detailed (default) or Brief audit log type as follows:

1. From the Grid tab, select the Grid Manager tab -> Members tab, and then click Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the General tab, and then select one of the following:
   - **Detailed**: This is the default type. When you select this, Grid Manager displays detailed information on all administrative changes such as the timestamp of the change, administrator name, changed object name, and the new values of all properties in the logged message.
   - **Brief**: Provides information on administrative changes such as the changed object name and action in the log message. The logged message does not show timestamp or admin name.

### Viewing the Audit Log

To view an audit log:

1. From the Administration tab, select the Logs tab -> Audit Log tab.
2. Optionally, use the filters to narrow down the audit log messages you want to view. Click Show Filters to enable the filters. Configure the filter criteria, and then click Apply.

   Based on your filter criteria (if any), Grid Manager displays the following in the Audit Log viewer:

   - **Timestamp**: The date, time, and time zone the task was performed. The time zone is the time zone configured on the member.
   - **Admin**: The admin user who performed the task.

   **Note**: The admin user displayed as $admin group name$ represents an internal user. You can create an admin filter with “matches expression” equals ^[^$] to filter out internal users.

   - **Action**: The action performed. This can be CALLED, CREATED, DELETED, LOGIN_ALLOWED, LOGIN_DECLINED, MESSAGE, and MODIFIED.
   - **Object Type**: The object type of the object involved in this task. This field is not displayed by default. You can select this for display.
   - **Object Name**: The name of the object involved in this task.
   - **Execution Status**: The execution status of the task. Possible values are Executed, Normal, Pending Approval and Scheduled.
   - **Message**: Detailed information about the performed task.

You can also do the following in the log viewer:

- Toggle between the single line view and the multi-line view for display.
- Navigate to the next or last page of the file using the paging buttons.
- Refresh the audit log view.
- Click the Follow icon to have the appliance automatically refresh the log every five seconds.
- Download the log.
- Clear the contents of the audit log.
- Use filters and the Go To function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
• Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
• Export or print the content of the log.

Searching in the Audit Log

Instead of paging through the audit log file to locate messages, you can have the appliance search for messages with certain text strings. To search for specific messages:

• Enter a search value in the search field below the filters, and then click the Search icon.

The appliance searches through the audit log file and highlights the search value in the viewer. You can use the arrow keys next to the Search icon to locate the previous or next message that contains the search value.

Downloading the Audit Log

You can download the audit log file to a specified directory, if you want to analyze it later. To download an audit log file:

1. From the Administration tab, select the Logs tab -> Audit Log tab, and then click the Download icon.
2. Navigate to a directory where you want to save the file, optionally change the file name (the default name is auditLog.tar.gz), and then click OK. If you want to download multiple audit log files to the same location, rename each downloaded file before downloading the next.

Note: If your browser has a pop-up blocker enabled, you must turn off the pop-up blocker or configure your browser to allow pop-ups for downloading files.

Viewing the Replication Status

The Replication Status panel reports the status of the database replication between Grid members and Grid Master, and between the two nodes in an independent HA pair. You can use this information to check the health of the Grid and HA pair activity.

To view the current replication status, from the Grid tab, select the Grid Manager tab -> Members tab, and then click Toggle Replication Status View.

Grid Manager can display the following replication information for each member:

• Name: The FQDN (fully qualified domain name) of the appliance.
• Send Queue: The size of the queue from the Grid Master to the Grid member.
• Last Send: The timestamp of the last replication information sent by the Grid Master.
• Receive Queue: The size of the queue from the Grid member to the Grid Master.
• Last Receive: The timestamp of the last replication information sent received by the Grid Master.
• Member Replication Status: The replication status between the member and the Grid Master. Grid Manager displays the status in green when the status is fine or red when the member is offline.
• HA Replication Status: The HA replication status between the active and passive nodes. The status is at the member level, not at the node level. Grid Manager displays the status in red when one of the nodes is offline.
• Status: The current operational status of the appliance. The status can be one of the following:
  • Green: The appliance is operating normally in a “Running” state.
  • Yellow: The appliance is connecting or synchronizing with its Grid Master.
  • Red: The Grid member is offline, is not licensed (that is, it does not have a DNSOne license with the Grid upgrade that permits Grid membership), is upgrading or downgrading, or is shutting down.
• IPv4 Address: The IPv4 address of the appliance or the VIP of an HA pair.
• IPv6 Address: The IPv6 address of the appliance or the VIP of an HA pair.
• Identify: This field appears only if your appliance has the unit identification button. This can be On or Off. When you identify the appliance by pressing the UID button on the appliance or through the GUI or CLI command, this field displays On. Otherwise, this is Off.
• DHCP, DNS, TFTP, HTTP, FTP, NTP, bloxTools, Captive Portal, DNS Accelerator Usage, Discovery, Reporting: The current status of the service. The status can be one of the following:
  • Green: The service is enabled and running properly.
  • Yellow: The service is enabled, but there may be some issues that require attention.
  • Red: The service is enabled, but it is not running properly. A red status icon can also appear temporarily when a service is enabled and begins running, but the monitoring mechanism has not yet notified the Infoblox GUI.
  • Gray: The service is not configured or it is disabled.
• Hardware Type: The hardware type of the appliance, such as IB-1400.
• Serial Number: The serial number of the appliance.
• DB Utilization: The percentage of the database that is currently in use.
• Comment: Information about the appliance.
• Site: The location to which the member belongs. This is one of the predefined extensible attributes.
• HA: Indicates whether the member is an HA pair. If the member is an HA pair, Grid Manager displays the status of the HA pair.
• Hardware Model: The hardware model of the appliance.

You can do the following:

• Use filters and the Go To function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an
Using the Traffic Capture Tool

You can capture the traffic on one or all of the ports on a NIOS appliance, and then view it using a third-party network protocol analyzer application, such as the Wireshark – Network Protocol Analyzer™. The NIOS appliance must have a minimum of 500 MB of free disk space to start the traffic capture; otherwise, the traffic capture might fail.

The NIOS appliance saves all the traffic it captures in a .cap file and compresses it into a .tar.gz file. Your management system must have a utility that can extract the .tar file from the .gzip file, and an application that can read the .cap (capture) file format. The size of the .cap file is limited to 4 GB for the Infoblox-4010, Infoblox-4030, Infoblox-4030-10GE, and PT-4000, and the size is limited to 1 GB for all other NIOS appliances. You can also transfer the traffic capture file to your local management system, a TFTP server, an FTP server, or a SCP server.

**Note:** This feature captures traffic of all the direct responses received from the cache accelerator on the IB-4030.

This section explains the process of capturing traffic, and how to download the traffic capture file to your management system. After that, you can extract the traffic capture file and view it with a third-party network protocol analyzer application. The traffic capture file is shared between NIOS admin users.

**Note:** The NIOS appliance always saves a traffic capture file as tcpdumpLog.tar.gz. If you want to download multiple traffic capture files to the same location, rename each downloaded file before downloading the next.

You can also capture traffic on the NIOS appliance through the Infoblox CLI using the `set traffic_capture` command. For more information, refer to the Infoblox CLI Guide. Grid Manager displays the traffic capture status and it allows you to download the captured traffic, irrespective of whether the traffic capture is initiated from the Infoblox CLI or from Grid Manager.

To capture traffic on a member:

1. From the Grid tab, select the Grid Manager tab -> Members tab, and then click Traffic Capture from the Toolbar.

2. In the Traffic Capture dialog box, complete the following:
   - **Member:** Grid Manager displays the selected member on which you want to capture traffic. If no member is displayed or if you want to specify a different member, click Select. When there are multiple members, Grid Manager displays the Member Selector dialog box from which you can select one. You cannot capture traffic on an offline member.
   - **Interface:** Select the port on which you want to capture traffic. Note that if you enabled the LAN2 failover feature, the LAN and LAN2 ports generate the same output. (For information about the LAN2 failover feature, see About Port Redundancy.)
     - **LAN:** Select this to capture all the traffic the LAN port receives and transmits.
     - **MGMT:** Select this to capture all the traffic the MGMT port receives and transmits.
     - **LAN2:** Select to capture all the traffic the LAN2 port (if enabled) receives and transmits.
     - **All:** Select this to capture the traffic addressed to all ports. Note that the NIOS appliance only captures traffic that is addressed to it.
     - **LANx nnnn:** If you have configured VLANs on the LAN1 or LAN2 port, the appliance displays the VLANs in the format LANx nnnn, where x represents the port number and nnnn represents the associated VLAN ID.

   **Note:** Riverbed virtual appliances support capturing traffic only on the LAN port.

   - **Seconds to run:** Specify the number of seconds you want the traffic capture tool to run.

3. **Capture Control:** Click the Start icon to start the capture. A warning message appears indicating that this report will overwrite the existing file. Click Yes. You can click the Stop icon to stop the capture after you start it.

4. **Transfer To:** Select the destination to transfer the traffic capture file. You can select My Computer, TFTP, FTP, or SCP from the drop-down list. Note that you cannot transfer the traffic capture file when the traffic capture is in progress.
   - **My Computer:** Transfer the traffic capture file to a local directory on your computer. This is the default.
   - **TFTP:** Transfer the traffic capture file to a TFTP server.
     - **Filename:** Enter the directory path and the file name of the traffic capture file. For example, you can enter /home/test/Infoblox_2016_03_01.
     - **IP Address of TFTP Server:** Enter the IP address of the TFTP server to which you want to transfer the traffic capture file.
   - **FTP:** Transfer the traffic capture file to an FTP server.
     - **Filename:** Enter the directory path and the file name of the traffic capture file. For example, you can enter /home/test/Infoblox_2016_03_01.
     - **IP Address of FTP Server:** The IP address of the FTP server.
• **Username**: Enter the username of your FTP account.
• **Password**: Enter the password of your FTP account.
• **SCP**: Transfer the traffic capture file to an SCP server.
• **Filename**: Enter the directory path and the file name of the traffic capture file. For example, you can enter `/home/test/Infoblox_2016_03_01`.
• **IP Address of SCP Server**: The IP address of the SCP server.
• **Username**: Enter the username of your SCP account.
• **Password**: Enter the password of your SCP account.

5. **Uncompressed Capture File Size**: Click **Download** to download the captured traffic after the capture stops and then save the file. You can rename the file if you want. You cannot download the traffic report when the tool is running. Grid Manager updates the size of the report when the capture tool is running.

**Note**: The NIOS appliance must have free disk space of at least 500MB + size of the traffic capture file (4 GB/1 GB, depending on the appliance model) to download the traffic capture file.

6. Use terminal window commands (Linux) or a software application (such as StuffIt™ or WinZip™) to extract the contents of the .tar.gz file.

7. When you see the traffic.cap file in the directory where you extract the .tar.gz file, open it with a third-party network protocol analyzer application.

### Using the Capacity Report

You can view the capacity usage and object type information of an appliance in a capacity report. The capacity report displays capacity and object type information of an independent appliance, a Grid Master, or a Grid member. For an HA pair, the report displays information on the active node.

The top half of the panel displays a capacity summary, and the bottom half displays the object types the appliance supports and the total counts for each object type.

To view a capacity report:

- From the **Grid** tab, select the **Grid Manager** tab -> **Members** tab -> **member** check box, and then click **Capacity Report** from the Toolbar.

The capacity summary contains the following information:

- **Name**: The name of the appliance.
- **Role**: The role of the appliance. The value can be **Grid Master**, **Grid Master Candidate**, **Grid Member**, or **Standalone**.
- **Hardware Type**: The type of hardware. For an HA pair, the report displays the hardware type for both the active and passive nodes.
- **Object Capacity**: The maximum number of objects the appliance can support.
- **Total Objects**: The total number of objects currently in the database.
- **% Capacity Used**: The percentage of the capacity in use.

The capacity report filters object types you can manage through the appliance. You can configure the object types you want to see in the following table by completing the following in the **Minimum Object Total** filter:

- **Minimum Object Total**: Enter the minimum number of objects within an object type of which Grid Manager displays. In the Object Type table, Grid Manager displays only the object types that contain at least the specified number of objects you enter in this field.

The capacity report displays the following information:

- **Object Type**: The type of objects. For example, DHCP Lease, Admin Group, or PTR Record. For objects that are only used for internal system operations, the report groups and shows them under **Other**.
- **Total**: The total number of objects for the specific object type. You can print the object type information or export it to a CSV file.

### Participating in the Customer Experience Improvement Program

Administrators with superuser accounts can configure a Grid Master or an independent appliance to email reports monthly and after each upgrade to Infoblox Technical Support and other specified recipients. The reports are also included in support bundles that you download.

The reports provide status and event information about the Grid or independent appliance and its services. The report is an XML document that includes the following information:

- The phone home feature version.
- The report type, such as periodic and test.
- The time of the report.
- The Infoblox Support ID that was assigned to the account.
- Information about the Grid, such as its NIOS version, name, VIP, Grid Master hostname, LAN IP, and the number of Grid members and appliances in the Grid.
- The upgrade history of the Grid.
- Information about each Grid member, such as the hostname, IP address, status, role (such as standalone, master), and if the member is
an HA pair. If the member is a peer in a DHCP failover association, the report also includes the DHCP failover status. 
- Hardware information, such as the hardware type, serial number, HA status, and uptime.
- Information about the interfaces, such as the interface name and IP addresses.
- Resource usage information, such as CPU and system temperature, and CPU, database, disk, and memory usage.

Note that if the appliance is configured to send email notifications to an SMTP relay server, as described in Notifying Administrators, the appliance sends the phone home reports to the relay server as well.

To configure the Grid Master to email status reports:

1. From the Grid tab, select the Grid Manager tab -> Members tab.
2. Expand the Toolbar and click Grid Properties -> Edit.
3. In the Grid Properties editor, select the Customer Improvement tab, and then complete the following:
   - Participate in Infoblox Customer Experience Improvement Program: Select the check box to send product usage data to Infoblox on a periodic basis. Infoblox uses this data to improve product functionality.
   - Support ID: Enter the Infoblox Support ID that was assigned to your account. It must be a number with four to six digits. Infoblox includes this ID in the data report.
   - Send notifications to:
     - Infoblox Support: Select this to email the reports to Infoblox Technical Support.
     - Additional email addresses: Optionally, you can specify up to 16 additional recipients. Click the Add icon and enter the email addresses of the recipients.
   - Send Test Report: Click this to send a test report to the specified recipients.
4. Save the configuration and click Restart if it appears at the top of the screen.

**Monitoring DNS Transactions**

The NIOS appliance provides tools for monitoring DNS transactions and mitigating cache poisoning from UDP (User Datagram Protocol) traffic on source port 53. Cache poisoning can occur when a DNS server accepts maliciously created unauthentic data. The DNS server ends up locally caching the incorrect entries and serving them to users that make the same DNS requests. In a maliciously created situation, the attacker can redirect Internet traffic from the legitimate host to another host that the attacker controls.

You can configure the appliance to track invalid DNS responses for recursive DNS queries. The appliance tracks DNS responses that arrive on invalid ports or have invalid TXIDs (DNS transaction IDs). Both invalid ports and invalid TXIDs could be indicators of cache poisoning. An invalid port is a DNS response that arrives from UDP (User Datagram Protocol) port 53 with either one of the following conditions:

- There are no outstanding DNS requests from the port on which the response arrives.
- The TXID of the DNS response matches the TXID of an outstanding request. However, the request was sent from a port other than the port on which the response arrives.

An invalid TXID is a DNS response that arrives from UDP port 53, and the TXID does not match the TXID of an outstanding DNS request. Figure 37.1 illustrates how the appliance detects an invalid port and an invalid TXID.

![Figure 37.1: Invalid Port and Invalid TXID](image-url)
Both invalid ports and invalid TXIDs could be indicators of DNS cache poisoning, although a small number of them is considered normal in situations where valid DNS responses arrive after the DNS queries have timed out. You can configure the appliance to track these indicators, and you can view their status. You can also configure thresholds for them. When the number of invalid ports or invalid TXIDs exceeds the thresholds, the appliance logs an event in the syslog file and sends an SNMP trap and e-mail notification, if you enable them. You can then configure rate limiting rules to limit incoming traffic or completely block connections from primary sources that send the invalid DNS responses.

Rate limiting is a token bucket system that accepts packets from a source based on the rate limit. You can configure the number of packets per minute that the Infoblox DNS server accepts from a specified source. You can also configure the number of packets for burst traffic, which is the maximum number of packets that the token bucket can accept. Once the bucket reaches the limit for burst traffic, it discards the packets and starts receiving new packets according to the rate limit.

The appliance monitors only UDP traffic from remote port 53 for the following reasons:

- The attacks that the appliance monitors do not happen over TCP.
- DNS responses are sent only from port 53. The appliance discards DNS responses that are sent from other ports.

To monitor invalid ports and invalid TXIDs on the Infoblox DNS server, follow these procedures:

1. Enable DNS network monitoring and DNS alert monitoring. For information, see Enabling and Disabling DNS Alert Monitoring.
2. Configure the thresholds for DNS alert indicators. For information, see Configuring DNS Alert Thresholds.
3. Enable SNMP traps and e-mail notifications. For information, see Configuring SNMP.
4. Review the DNS alert status. For information, see Viewing DNS Alert Indicator Status.
5. Identify the source of the attack by reviewing the DNS alert status, syslog file, and SNMP traps. For information on SNMP traps for DNS alerts, see Threshold Crossing Traps.

To mitigate cache poisoning, you can limit incoming traffic or completely block connections from specific sources, as follows:

- Enable rate limiting on the DNS server. For information, see Enabling and Disabling Rate Limiting from External Sources.
- Configure rate limit traffic rules from specific sources. For information, see Configuring Rate Limiting Rules.

You can verify the rate limiting rules after you configure them. For information, see Viewing Rate Limiting Rules.

### Enabling and Disabling DNS Alert Monitoring

The appliance monitors only UDP traffic on port 53 for recursive queries, and then reports invalid DNS responses. DNS alert monitoring is disabled by default. For an HA pair, you must enable DNS alert monitoring on both the active and passive nodes.

To enable DNS network monitoring and DNS alert monitoring:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```
   set monitor dns on
   ```
   The appliance displays the following:
   ```
   Turning on DNS Network Monitoring...
   ```
3. Enter the following command:
   ```
   set monitor dns alert on
   ```

When you enable DNS alert monitoring and DNS network monitoring is disabled, the appliance automatically enables DNS network monitoring and displays the following:

```
DNS Network Monitoring is disabled. It must be enabled for alerting to function.
Enable DNS Monitoring now? (y or n):
```

You can also disable DNS network monitoring and DNS alert monitoring using the following commands:

```
set monitor dns off
set monitor dns alert off
```

**Note:** When you restart DNS network monitoring, you also reset the SNMP counters for DNS alerts.

You can then view the alert status to identify the primary source of invalid DNS responses. For information, see [bookmark2831](#).

### Viewing DNS Alert Indicator Status

To view DNS alert indicator status:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```
   show monitor dns alert status
   ```
The appliance displays historical alert counts and up to five primary sources that generate invalid DNS responses, as shown in the following example:

Data last updated: Mon Oct 6 14:47:12 2008

DNS Alert
1m | 5m | 15m | 60m | 24h | Ever
--------------------------------------------
port 12 | 12 | 12 | 12 | 12 | 12
txid 12 | 12 | 12 | 12 | 12 | 12

There were 80 DNS responses seen in the last minute.
10% were to an invalid port.
10% had an invalid TXID.

Primary sources of invalid responses:
4.4.4.4 (unknown) sent 4
2.2.2.2 (unknown) sent 3
7.7.7.7 (unknown) sent 1

The appliance attempts to resolve the hostnames of the sources that sent invalid responses, if the DNS resolver is enabled. If the appliance cannot resolve a hostname, it displays "unknown" as the hostname of the invalid response.

Configuring DNS Alert Thresholds

You can configure thresholds for DNS alerts to control when the appliance tracks DNS attacks on UDP port 53 and issues SNMP traps and e-mail notifications.

Note: Ensure that you enable SNMP traps and e-mail notifications. For information, see Configuring SNMP.

You can configure thresholds for both invalid ports and invalid TXIDs. The default thresholds for both invalid ports and TXIDs are 50%. When the number of invalid ports or invalid TXIDs exceeds the thresholds, the appliance logs the event and sends SNMP traps and notifications. You can configure the thresholds either as absolute packet counts or as percentages of the total traffic during a one minute time interval.

To configure DNS alert thresholds:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:

   set monitor dns alert modify port | txid over threshold_value packets | percent

   where
   port | txid = Enter port to set the threshold for invalid ports, or enter txid to set the threshold for invalid TXIDs.
   threshold_value = Enter the number of packets or percentage for the threshold.
   packets | percent = Enter packets if you want to track the total packet count, or enter percentage if you want to track a percentage of the total traffic. For a percentage-based threshold, the appliance does not generate a threshold crossing event if the traffic level is less than 100 packets per minute.

   For example, if you want the appliance to send a DNS alert when the percentage of DNS responses arriving on invalid ports from UDP port 53 exceeds 70% per minute, you can enter the following command:

   set monitor dns alert modify port over 70 percent

   If you want the appliance to send a DNS alert when the total number of packets with invalid TXIDs from UDP port 53 is over 100 packets per minute, you can enter the following command:

   set monitor dns alert modify txid over 100 packets

   When there is a DNS alert, the appliance logs an event in the syslog file and sends an SNMP trap and e-mail notification if enabled.

Viewing DNS Alert Thresholds

You can view the DNS alert thresholds. The appliance displays the current thresholds. If you have not configured new thresholds, the appliance displays the default thresholds, which are 50% for both invalid port and TXID.

To view the DNS alert thresholds:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
show monitor dns alert

The appliance displays the threshold information as shown in the following example:

DNS Network Monitoring is enabled. Alerting is enabled.
DNS Alert Threshold (per minute)
---------------------------------------------
portover 70% of packets
trans over 100 packets

Enabling and Disabling Rate Limiting from External Sources

You can mitigate cache poisoning on your DNS server by limiting the traffic or blocking connections from UDP port 53. To enable rate limiting from sources:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```
   set ip_rate_limit on
   ```
   The appliance displays the following:
   Enabling rate limiting will discard packets and may degrade performance.
   Are you sure? (y or n):

   Note: When you enable rate limiting, the appliance discards packets based on the configured rate limiting rules. This might affect the DNS performance when the appliance discards valid DNS responses.

3. Enter y to enable rate limiting.

When you enable rate limiting, the appliance applies the rate limiting rules that you configured. You might want to configure the rate limiting rules before enabling rate limiting. For information on how to configure rate limiting rules, see bookmark2834. You can also disable rate limiting by entering the following command:

   ```
   set ip_rate_limit off
   ```

When you disable rate limiting, the appliance stops applying the rate limiting rules.

Configuring Rate Limiting Rules

You configure rate limiting rules to limit access or block connections from UDP port 53. The rules take effect when you enable rate limiting. When adding rules, ensure that you do not include an IP address that matches the IP address of either the Grid Master or Grid member. Doing this could affect VPN connectivity. To configure rate limiting rules:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   ```
   set ip_rate_limit add source all | ip_address [/mask] limit packets/m [burst burst_packets]
   ```
   where
   - all | ip_address = Enter all or 0.0.0.0 if you want to limit all traffic from all sources, or enter the IP address from which you want to limit the traffic.
   - [/mask] = Optionally, enter the netmask of the host from which you want to limit the traffic.
   - packets = Enter the number of packets per minute that you want to receive from the source.
   - [burst burst_packets] = Optionally, enter burst and the number of packets for burst traffic. This is the maximum number of packets accepted.

The following are sample commands and descriptions for rate limiting rules:

- To block all traffic from host 10.10.1.1, enter the following command:
  ```
  set ip_rate_limit add source 10.10.1.1 limit 0
  ```
- To limit traffic to five packets per minute from host 10.10.1.2, enter the following command:
  ```
  set ip_rate_limit add source 10.10.1.2 limit 5/m
  ```
To limit the traffic to five packets per minute from host 10.10.2.1/24 with an allowance for burst traffic of 10 packets, enter the following command:

```
set ip_rate_limit add source 10.10.2.1/24 limit 5/m burst 10
```

To limit the traffic to 5000 packets per minute from all sources, enter the following command:

```
set ip_rate_limit add source all limit 5000/m
```

Removing Rate Limiting Rules

You can remove the existing rate limiting rules that limit access or block connections from UDP port 53. To remove all the existing rules:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:
   
   - To remove the rate limiting rule that limits traffic from all sources, enter:
     
     ```
     set ip_rate_limit remove source all
     ```
   
   or
   
   - To remove all of the rate limiting rules from all sources, enter:
     
     ```
     set ip_rate_limit remove all
     ```

To remove one of the existing rules for an existing host:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:

   ```
   set ip_rate_limit remove source ip-address[/mask]
   ```

Viewing Rate Limiting Rules

You can view the existing rate limiting rules that limit access or block connections from UDP port 53. To view rate limiting rules:

1. Log in to the Infoblox CLI as a superuser account.
2. Enter the following CLI command:

   ```
   show ip_rate_limit
   ```

   The appliance displays the rules, as shown in the following example:

   IP rate limiting is enabled.

<table>
<thead>
<tr>
<th>Source</th>
<th>Limit</th>
<th>Burst</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.1.1</td>
<td>0 packets/minute</td>
<td>0 packets</td>
</tr>
<tr>
<td>10.10.1.2</td>
<td>5 packets/minute</td>
<td>5 packets</td>
</tr>
<tr>
<td>10.10.2.1/24</td>
<td>5 packets/minute</td>
<td>10 packets</td>
</tr>
<tr>
<td>all</td>
<td>5000 packets/minute</td>
<td>5000 packets</td>
</tr>
</tbody>
</table>

Tracking Object Changes in the Database

If you have external applications that use information in the NIOS database, you can use the Object Change Tracking feature to get informed about changes in the NIOS database. You can then periodically synchronize IPAM, DNS, and DHCP data through the Infoblox API or RESTful API, which returns updated object information. When you enable this feature, the appliance tracks the changes that are made to NIOS objects. It assigns sequence IDs to all the changed objects. These sequence IDs are incremented when there is a change in the high-level objects such as IPv4 and IPv6 fixed addresses, networks, network containers, and others. When you query using the `db_objects` through the Infoblox API for desired object types, the application returns all the objects of those object types that changed after the sequence ID given in the query.

When you enable the Object Change Tracking feature, you can also specify the lifetime of deleted objects in the database and the total number of objects that must be present in the database. The deleted objects that are saved in the database are purged periodically. Note that you cannot track the user who created or updated an existing object.

Infoblox supports full and incremental synchronization for these changes. Certain events such as Grid Master Candidate promotions and upgrades require a full synchronization.

Users with read-only permission can use this feature. For more information, see [Administrative Permissions for Object Change Tracking](#). To enable and use the Object Change Tracking feature to track and synchronize updates, complete the following:
1. Enable the feature, as described in Enabling Object Change Tracking.
2. Select whether you want to use a full synchronization or an incremental synchronization. When you use one of these synchronization methods to synchronize data through Infoblox API or RESTful API, they return updated objects that can be used to update your relational database. For full synchronization, see Using Full Synchronization. For incremental synchronization, see Using Incremental Synchronization.

Best Practices for Object Change Tracking

- The Object Change Tracking feature is optimized to reduce impact on the DDI services and it runs only on the Grid Master. The synchronization process synchronizes 1000 objects at a time with a 2 second pause in between. There might be a slight impact on the Grid Master Candidate as they get updates from the Grid Master. When protocol services are running on the Grid Master Candidate you might encounter a 5% drop in the protocol performance. This feature does not impact the services that are running on the Grid members.
- NIOS does not update the sequence ID of the respective parent when you modify a child object. For example, inserting an A record under DNS zone does not increase the sequence number of the zone object.
- When you delete a parent object, NIOS saves the child objects in the deleted object table. But, if the associated child objects are either resource records or leases, NIOS will neither save them in the deleted object table nor update the sequence ID for these child objects.
- If you update a parent object, then the sequence ID of its child objects will not change.
- NIOS updates the sequence ID of the host record and IPv4 and IPv6 host addresses, if there are any changes to host addresses, both IPv4 and IPv6. The sequence ID is also updated when you update the host alias records that results in increase in the sequence ID of the host record and all its child objects.

For example, if you create a host record hhh.test.com with an IPv4 address and perform an incremental synchronization to get updates, the response contains an updated host record and host address:

curl -k1 -u admin:infoblox -H content-type:application/json -X GET https://10.32.2.202/wapi/v2.5/db_objects?start_sequence_id=2830689052:0\&object_types=record:host,record:host_ipv4addr\&_return_fields=last_sequence_id,object,object_type\;_return_type=json-pretty

The response is as follows:

```json
[
  {
    "_ref": "db_objects/Li5hbGxfY2hhbmdl12F9vYmp1Y3RzJDIw:38",
    "object": {
      "_ref": "record:host/ZG5zLmhvc3QkL19kZWZhdWx0OlNvbS5rYXJqYVdpLmhvc3Qx:hhhtest.com/default",
      "ipv4addrs": [{
        "_ref": "record:host_ipv4addr/ZG5zLmhvc3RfYWRkcmVzcyQuX2RlZmF1bHQuY29tLmthcmphZ2kuaG9zdDEuMS4xLjEuM54:1.1.1.1/ hhh.test.com/default",
        "configure_for_dhcp": false,
        "host": " hhh.test.com",
        "ipv4addr": "1.1.1.1",
        "mac": "11:11:11:11:11:11"
      }],
      "ipv6addrs": [{
        "_ref": "record:host_ipv6addr/ZG5zLmhvc3RfYWRkcmVzcyQuX2RlZmF1bHQuY29tLmthcmphZ2kuaG9zdDEuM54:OmFhLg:aa%3A%3Aaa/ hhh.test.com/default",
        "configure_for_dhcp": false,
        "host": " hhh.test.com",
        "ipv6addr": "aa::aa"
      }],
      "name": " hhh.test.com",
      "view": "default"
    },
    "object_type": "record:host",
    "unique_id": "c326fcf8058c4022939050af96a0fdb2"
  },
  {
    "_ref": "db_objects/Li5hbGxfY2hhbmdl12F9vYmp1Y3RzJDIw:38",
    "object": {
  ```
When you update DNS host, host address, and host alias, NIOS updates the sequence IDs of child objects associated with these parent objects even though the changes do not affect the child objects. For example, when you update an existing comment in the host record, NIOS updates the sequence IDs of child objects associated with the respective host record.

Example:

```
curl -k -u admin:infoblox -H content-type:application/json -X GET https://10.32.2.202/wapi/v2.5/db_objects?start_sequence_id=2830689052:0&object_types=record:host,record:host_ipv4addr&_return_fields=last_sequence_id,object,object_type,object.comment&_return_type=json-pretty
```

The response is as follows:

```json
[
   {
      "_ref": "db_objects/Li5hbGxfY2hhbmd1ZFWyMmp1Y3RzJD1y:27",
      "object": {
         "_ref": "record:host/ZG5zLmhc3RfYWRkcmVzcyQuX2RlZmF1bHQuY29tLmthcmphZ2kuaG9zdDEuYWE6OmPhLg:aa%3A%3Aaa/hhh.test.com/default",
         "configure_for_dhcp": false,
         "host": "hhh.test.com",
         "ipv6addr": "aa::aa"
      },
      "object_type": "record:host_ipv6addr",
      "unique_id": "2b19a399c3f747538d879fdd33a4de32"
   },
   {
      "_ref": "db_objects/Li5hbGxfY2hhbmd1ZFWyMmp1Y3RzJD1y:38",
      "object": {
         "_ref": "record:host_ipv4addr/ZG5zLmhc3RfYWRkcmVzcyQuX2RlZmF1bHQuY29tLmthcmphZ2kuaG9zdDEuMS4xLjEuMS41.1.1.1/hhh.test.com/default",
         "configure_for_dhcp": false,
         "host": "hhh.test.com",
         "ipv4addr": "1.1.1.1",
         "mac": "11:11:11:11:11"
      },
      "object_type": "record:host_ipv4addr",
      "unique_id": "3fb8fba003d647ceac5796a28459725a"
   },
   {
      "_ref": "db_objects/Li5hbGxfY2hhbmd1ZFWyMmp1Y3RzJD1z:3956302770%3A38",
      "last_sequence_id": "3956302770:38"
   }
]
```
When an IPv4 or an IPv6 host address changes, NIOS deletes the old record and creates a new record with the updated IP address. Note that new sequence IDs are generated for the associated objects. When you query a host record, NIOS displays the list of host addresses associated with it.

Example:

curl -k -u admin:infoblox -H content-type:application/json -X GET https://10.32.2.202/wapi/v2.5/db_objects?start_sequence_id=2830689052:0\&object_types=record:host,record:host_ipv4addr\;_return_fields=last_sequence_id,object,object_type\;_return_type=json-pretty

The response is as follows:

```json
[
  {
    "_ref": "db_objects/Li5hbGxfY2hhbmdl1ZF9vYmplY3RzJDQ:28",
    "last_sequence_id": "2830689052:27"
  }
]
```

- NIOS returns the shared records per zone when you query for them. For example, consider two zones, z1 and z2, and a shared record group, srg1, which contains a shared record sr1. The shared record group srg1 is associated with the zones z1 and z2. Hence, the
shared record sr1 is shared between two zones, z1 and z2, but NIOS saves only a single copy of the shared record sr1 in the database. When you query for shared record updates, NIOS returns two records for z1 and z2, as sr1 is associated with both the zones, z1 and z2, and saves these records with a UUID and a sequence ID in the table. The response also contains new records with zone pointing to the zone it belongs to, UUID and sequence ID of the new records and a shared record group, which indicates that it is a shared record and not a normal resource record. When you enable Object Change Tracking feature, NIOS clears this table and recreates a new table for the existing shared records.

- Note that NIOS generates two leases in the database when a client sends a DHCP request to the NIOS DHCP server, which is configured with failover association. You can perform either a full or an incremental synchronization in this scenario. Infoblox recommends that you ignore the lease that is generated by the failover DHCP server with binding_state as BACKUP and consider the lease with binding_state as ACTIVE.
- File distribution service automatically removes old files from wapi_output directory if there is no sufficient space for new files. NIOS allocates 50% of each of the file distribution area to wapi_output directory and normal files. For example, if the file distribution area is allocated 500 MB, then 250 MB is used for wapi_output directory and the remaining 250 MB is used for normal files.
- NIOS does not support WAPI paging mechanism. As the synchronization results are displayed in the order of sequence_id, you must specify _max_results to achieve paging mechanism for synchronization.
- NIOS deletes all previous scheduled tasks after a restore or an upgrade operation.

### Enabling Object Change Tracking

To enable object change tracking:

1. From the Grid tab, select the Grid Manager tab -> Members tab, and then click Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, click Object Change Tracking and complete the following:
   - Enable Object Change Tracking: Select this check box to enable object change tracking for the objects.
   - Status: Indicates whether object change tracking is enabled or not. You can view what percentage of the operation is complete.

**Note:** This operation might take a longer time to complete when you have a large database. For example, 1 million objects on an IB-4010 appliance takes approximately 1 hour. Infoblox recommends that you enable this feature during off-peak hours.

- **Maximum number of deleted objects that will be tracked:** Specify the total number of deleted objects that must be present in the database. The minimum value is 2,000 and the maximum value is 20,000. The default value is 4,000.
- 3. Save the configuration.

### Using Full Synchronization

Full synchronization synchronizes the entire set of objects irrespective of updates. You can perform a full synchronization only on the Grid Master and Grid Master Candidate. Note that the tasks created on the Grid Master and Grid Master Candidates will be executed on them respectively and you can download the synchronized data on to the member where the task was created. The Grid Master Candidate can execute only read-only tasks. To save the output of a full synchronization, you must specify the output location. The output of a full synchronization is in the following formats: JSON, XML, ROWJSON, or ROWXML.

You can specify one of the following output locations: "FILE_DISTRIBUTION" and "LOCAL".

- When _output_location = "FILE_DISTRIBUTION"

When you set the output location as mentioned above, you must specify a file name or a prefix for the file. NIOS saves the output file in the file distribution area and displays an error message if you do not specify a file name or a prefix. For more information about file distribution area, see Managing Directories.

When you select the above output location for a Grid Master Candidate, you must select Allow Upload to Grid Members to upload files to the file distribution area. Infoblox recommends that you use the Grid Master Candidate to offload the Grid Master. You must enable a full synchronization during off-peak hours if protocol services are running on the Grid Master Candidate. For more information, see Enabling Upload to Grid Members.

**Example:**

```bash
curl -k1 -u admin:infoblox -X POST 'https:..../wapi/v2.5/fileop?_function=read' -H 'Content-Type: application/json; charset=UTF-8' -d '{"_filename": "test.json", 
"_output_location": "FILE_DISTRIBUTION", 
"object": "db_objects", 
"all_object_types_supported_in_version": "2.5", 
"_encoding": "ROWJSON"}'
```

You can specify either _object = db_objects or all_object_types_supported_in_version=2.5 to retrieve all objects. When you specify _object = db_objects, NIOS returns only standard Restful API fields as response. To retrieve all fields of all objects, you can specify all_object_types_supported_in_version=2.5. To fetch the output file, start file distribution service and use the following URL:

```bash
curl -k1 -u admin:infoblox -X GET http://<ipaddress>/wapi_output/test.json -H 'Content-Type:application/json'
```

- When _output_location = "LOCAL"
If you schedule a full synchronization and set the output location as mentioned above, a file name is generated based on the task ID and the output file is saved at another location. You do not have to specify a file name or a prefix.

If you do not schedule a synchronization, then NIOS returns an URL and a token, which is used for the download complete function, in the response.

If you do not specify an output location, NIOS saves the file in the file distribution area.

Use the above output location for saving full synchronization files when file distribution area does not have enough space for storage.

Example:

```bash
curl -k1 -u admin:infoblox -X POST 'https://127.0.0.1/wapi/v2.5/fileop?_function=read&_schedinfo.schedule_now=true' -H 'Content-Type: application/json; charset=UTF-8' -d '{"_output_location": "LOCAL", "_object": "db_objects", "all_object_types_supported_in_version": "2.5", "_encoding": "JSON"}'
```

NIOS saves the output file in the file distribution area if you do not specify an output location as shown in the code below:

```bash
curl -k1 -u admin:infoblox -X POST 'https://127.0.0.1/wapi/v2.5/fileop?_function=read' -H 'Content-Type: application/json; charset=UTF-8' -d '{"_filename": "test.json", "_output_location": "FILE_DISTRIBUTION", "_object": "db_objects", "all_object_types_supported_in_version": "2.5", "_encoding": "ROWJSON"}'
```

Note the following about full synchronization:

- A full synchronization is required initially for a complete snapshot of the database.
- Depending on the size of requested data, a full synchronization may take a longer time to complete. For example, when 1 million objects are requested with all fields on an IB-4010 appliance, full synchronization takes a couple of hours. When 1 million objects are requested with standard RESTful API fields on an IB-4010 appliance, full synchronization takes less than an hour.
- Infoblox recommends that you request only object types with standard RESTful API fields and specify any additional required fields during a full synchronization.
- To dump full synchronization updates into a file using fileop->read operation when the updated objects are large in number, you can specify _object=db_objects and all the necessary parameters.
- Infoblox recommends a full synchronization in the following cases:
  - After an upgrade, restore or master promotion, which resets the sequence ID.
  - During off-peak hours for busy Grids with high rate of change that is greater than 500/sec.
  - When the maximum time or maximum number to track deleted objects is met, with the default being 4 hours and 4000 objects, then synchronization API returns an error if the last deleted sequence ID is newer than the current sequence ID.

Following are a few samples of API requests for full synchronization:

- If you specify _output_location = "local" and schedule the task, then you must use fileop ->get_file_url to retrieve the URL:

  ```bash
curl -k1 -u admin:infoblox -X POST 'https://127.0.0.1/wapi/v2.5/fileop?_function=get_file_url' -H 'Content-Type: application/json' -d '{"task_id":1}'
  ```

  The response is as follows:

  ```json
  "url": "https://10.32.2.202/http_direct_file_io/req_id-OBJECTS-1/nios-db-objects-1.JSON"
  ```

  You can fetch this file using the following API request:

  ```bash
  ```

- If you specify _output_location = "local" and do not schedule the task, then NIOS returns an URL and a token:

  ```bash
curl -k1 -u admin:infoblox -X POST 'https://127.0.0.1/wapi/v2.5/fileop?_function=read' -H 'Content-Type: application/json; charset=UTF-8' -d '{"_output_location": "LOCAL", "_object": "db_objects", "all_object_types_supported_in_version": "2.5", "_encoding": "JSON"}'
  ```

  The response is as follows:

  ```json
  {"token": "eJy1kU1vwyAMhu/8kfaWwG9C3nRpev6M0KzN5krmAQYhWhDg9Cm0AbmSzU3mKhb45\nn0Q4QXto2XVsxyT RkKYVFUoqqgqUBk+f1lknkR8BnWbHOLOMbp6nZZKtzG2ymAKP1FyAM44a0G8aT\n\q8USXd437T\n113O85x5l1
P1AB2eCevTS518eERURuCrBGsyzp3N1KTFyU+jaM3JRUOQ59a\rv5FpF\nk6nUixz8mWwStJfPb09u7n/64vyHCdp Ig9BcYrygPb2x1D+Gq5XwanyOOhu87KB48Mummvw9FX\n\nET+BNyT10D+A4+YAn3ryaE20tWzvh/QLT4Gbhw=", "url": "https://10.35.6.87/http_direct_file_io/req_id-DOWNLOAD-1001/nios-db-objects-09-05-20"
  ```
To save the file in a local area instead of the file distribution area:

curl -k -u admin:infoblox -X POST
'https://127.0.0.1/wapi/v2.5/fileop?_function=read&_schedinfo.schedule_now=true' -H 'Content-Type: application/json; charset=UTF-8' -d '{"_output_location": "LOCAL", "_object": "db_objects", "all_object_types_supported_in_version": "2.5", "_encoding": "JSON"}'

The response is as follows:
scheduledtask/b25lLnF1ZXV1Z90YXNzJDE:1/WAITING_EXECUTION

You can also schedule a full synchronization task as follows:

curl -k -u admin:infoblox -X POST
'https://127.0.0.1/wapi/v2.5/fileop?_function=read&_schedinfo.schedule_now=true' -H 'Content-Type: application/json; charset=UTF-8' -d '{"_filename": "test2.txt", "_object": "db_objects", "all_object_types_supported_in_version": "2.5", "_encoding": "JSON"}'

scheduledtask/b25lLnF1ZXV1Z90YXNzJDE:1/WAITING_EXECUTION

NIOS returns the scheduled task reference so that you can query and find out when will the scheduled task be complete:

curl -k -u admin:infoblox -X GET
https://127.0.0.1/wapi/v2.5/scheduledtask/b25lLnF1ZXV1Z90YXNzJDE:1/WAITING_EXECUTION

The response is as follows:
{
"_ref": "scheduledtask/b25lLnF1ZXV1Z90YXNzJDE:1/COMPLETED", "approval_status": "NONE", "execution_status": "COMPLETED", "task_id": 1
}

Note that the result is in either JSON or XML format. You can fetch the output file from the wapi-output directory of the file distribution area when the scheduled task is complete.

Using Incremental Synchronization

Incremental synchronization synchronizes only those objects that are updated since the previous synchronization. With incremental synchronization, you can query NIOS for any updates and when updates are found, NIOS returns the changed objects since the previous incremental synchronization. Incremental synchronization synchronizes the NIOS database for object changes such as addition, updates, or deletion, mostly via scripts. The incremental synchronization query consists of object types, a cookie of the form <id of db:sequence_id>, a sequence ID and an optional exclude_deleted object to indicate if the deleted objects must be excluded from the results. NIOS includes the deleted records in the results by default.

Note: Infoblox recommends that you use fileop->read for incremental synchronization when the updated objects are large in number.

Note the following about incremental synchronization:

- You cannot request an incremental synchronization to get updated (created, updated or deleted) objects after a full synchronization.
- For performance reasons, NIOS returns the objects that changed and not the object data that changed. Infoblox recommends that you figure out what changed by comparing the object with the previous version in the client database.
- Incremental synchronization may take a longer time to complete depending on the number of changes. For example, if 50K objects are requested with all fields on an IB-4010 appliance, an incremental synchronization approximately takes 2 minutes. When 50K objects are requested with standard RESTful API fields on an IB-4010, the synchronization process completes in approximately 1 minute.
- The size of the memory increases when the number of objects increases. Infoblox recommends that you use _max_results to limit the number of results or use the asynchronous fileop->read operation.
- Infoblox recommends that for a busy Grid with a high Rate of Change that is greater than 500/sec, you must run an incremental synchronization more frequently. Example: If the expected Rate of Change for objects in the Grid is 50/sec, you can schedule an incremental synchronization every 5-10 minutes. If the Rate of Change for objects is 200/sec, schedule an incremental synchronization every minute or every 2 minutes.
- Infoblox recommends that you include all object types when you query using an incremental synchronization, so that it returns the highest sequence ID for all objects that can be used for subsequent incremental updates. If you query only selected object types such as A record and zone, NIOS returns the highest sequence ID for those object types only.
- Consider an example where A record, Network, and A record are the object types with sequence ID 4, 5 and 6 respectively. When you query for an A record object type with a previous sequence ID using incremental synchronization, NIOS returns A record with the highest sequence ID, which is 6 and does not return the network object. Meanwhile, if you add or update a network object, then in the subsequent incremental synchronization it does not return the network object and you will lose updates made to the network object. Hence, Infoblox recommends that you include all object types in the query to ensure that you do not lose updates made to other object types.
- You cannot perform a full or an incremental synchronization during Grid Master Candidate promotions, restores, and upgrades.
The output of an incremental synchronization is either in JSON or XML format.

The following are a few samples of API requests for incremental synchronization:

- To get updates with all_objects_supported_in_version=2.5:

  ```
  curl -k1 -u admin:infoblox -H content-type:application/json -X GET
  https://10.35.6.87/wapi/v2.5/db_objects?start_sequence_id=992684967:0\&all_object_type
  s_supported_in_version=2.5\;return_fields=last_sequence_id,object,object_type,unique_id\;_return_type=json
  ```

  The response for the above API request contains all fields of all object types.

- To get an A record and an auth zone object update:

  ```
  curl -k1 -u admin:infoblox -H content-type:application/json -X GET
  https://10.32.2.202/wapi/v2.5/db_objects?start_sequence_id=183566281:0\&object_types=record:a,zone_aut
  h\;return_fields=last_sequence_id,object,object_type,unique_id\;_return_type=json
  ```

  The response is as follows:

  ```
  [{
    "_ref": "db_objects/Li5hbGxfY2hhbmd1ZF9vYmp1Y3RzJDA:19",
    "object": {
      "_ref": "zone_auth/ZG5zLnpvbmUkL19kZWZhdWxkOlNvbS5sZmFsb28:foo.com/default",
      "fqdn": "foo.com",
      "view": "default",
      "object_type": "zone_auth",
      "unique_id": "087af628fa03418fa057bb953807efc",
      "_ref": "db_objects/Li5hbGxfY2hhbmd1ZF9vYmp1Y3RzJDA:19",
      "object": {
        "_ref": "record:a/ZG5zLmJpbmRfYSQuX2RlZmF1bHQuY29tLmZvbyxhcmVJMSwxLmJibGVkVJMsLW5jb25zaW5lc3NhZ2U:arecl.fo",
        "ipv4addr": "1.2.3.2",
        "name": "arecl.fo.com",
        "view": "default",
        "object_type": "record:a",
        "unique_id": "89314c3fae2841f49600e1b66b0c7b7",
        "_ref": "db_objects/Li5hbGxfY2hhbmd1ZF9vYmp1Y3RzJDA:19",
        "last_sequence_id": "183566281:21"
      }
    }
  }
  ]
  ```

- NIOS returns deleted objects as synthetic deleted objects. To get updates on deleted host objects:

  ```
  curl -s -k1 -u admin:infoblox -H content-type:application/json -X GET
  https://10.34.19.220/wapi/v2.5/db_objects?start_sequence_id=1207501969:0\&object_types=record:host,bulkhost,record:host_ipv4addr,record:host_ipv6addr\&exclude_deleted=false
  ```

  The response is as follows:

  ```
  [{{
    "_ref": "db_objects/Li5hbGxfY2hhbmd1ZF9vYmp1Y3RzJDAQ:130",
    "object": {
      "_ref": "deleted_objects/Li5kZWxlZGl0b3JvZ29iamVjcmV0MQ",
      "object_type": "host_ipv6addr",
      "unique_id": "7a5e0622ed9db41ca47c12ca30700d5"
    },
    "object_type": "deleted_objects",
    "unique_id": "7a5e0622ed9db41ca47c12ca30700d5"
  }},
  {"_ref": "db_objects/Li5hbGxfY2hhbmd1ZF9vYmp1Y3RzJDM2Yw:130",
    "object": {
      "_ref": "deleted_objects/Li5kZWxlZGl0b3JvZ29iamVjcmV0MQ",
      "object_type": "host_ipv4addr",
      "unique_id": "6831685360001f38e8e134628ce62"
    },
    "object_type": "deleted_objects",
    "unique_id": "6831685360001f38e8e134628ce62"
  }],
  {"_ref": "db_objects/Li5hbGxfY2hhbmd1ZF9vYmp1Y3RzJDM2YQ:130",
    "object": {
      "_ref": "deleted_objects/Li5kZWxlZGl0b3JvZ29iamVjcmV0MQ",
      "object_type": "host_ipv6addr",
      "unique_id": "7a5e0622ed9db41ca47c12ca30700d5"
    },
    "object_type": "deleted_objects",
    "unique_id": "7a5e0622ed9db41ca47c12ca30700d5"
  }]
  ```

- To dump incremental synchronization updates into a file using fileop->read operation when the updated objects are large in number, you can specify _object=db_objects and all the necessary parameters for incremental synchronization:

  ```
  curl -k1 -u admin:infoblox -X POST 'https://10.34.19.100/wapi/v2.5/fileop?_function=read' -H 'Content-Type: application/json; charset=UTF-8' -d '{"_output_location": "LOCAL", "object": "db_objects", "start_sequence_id": "1973553522:0", "all_object_types_supported_in_version": "2.5", "max_results": 1000000, "encoding": "JSON"}'
  ```

For more information about supported objects in the Infoblox API and Restful API, refer to the Infoblox API Documentation and the Infoblox WAPI.
Syslog is a widely used mechanism for logging system events. NIOS appliances generate syslog messages that you can view through the Syslog viewer and download to a directory on your management station. In addition, you can configure a NIOS appliance to send the messages to one or more external syslog servers for later analysis. Syslog messages provide information about appliance operations and processes. NIOS appliances include syslog messages generated by the bloxTools service. You can choose logging categories to send specific syslog messages. The prefixes in the syslog messages are based on the logging categories you configure in the syslog. Note that syslog messages are prefixed only when you select logging categories. For information about how to configure logging categories, see 4817325. You can also include audit log messages and specific BIND messages among the messages the appliance sends to the syslog server.

In addition to saving system messages to a remote syslog server, a NIOS appliance also stores the system messages locally. When the syslog file reaches its maximum size, which is 300 MB for Infoblox appliances and VMware virtual appliances, and 20 MB for Riverbed virtual appliances, the appliance automatically writes the file into a new file by adding a .0 extension to the first file and incrementing subsequent file extensions by 1. Files are compressed during the rotation process, adding .gz extension following the numerical increment (file.4.gz). The sequential incrementation goes from zero through nine. When the eleventh file is started, the tenth log file (file.9.gz) is deleted, and subsequent files arerenumbered accordingly. For example, the current log file moves to file.0.gz, the previous file.0.gz moves to file.1.gz, and so on through file.9.gz. A maximum of 10 log files (0-9) are kept.

You can set syslog parameters at the Grid and member levels. At the member level, you can override Grid-level syslog settings and enable syslog proxy. You can configure the appliance to back up rotated syslog files to external servers through FTP or SCP. When you do so, the appliance forwards the rotated syslog files to the external servers that you configure. You can configure up to 10 external syslog backup servers each at the Grid and member levels. You can also override the Grid-level server configuration at the member level. For information about configuring syslog backup servers, see 4817325 4817325.

This section includes the following topics:

- 4817325
- 4817325
- 4817325
- 4817325
- 4817325
- 4817325
- Downloading the Audit Log

Specifying Syslog Servers

To configure a NIOS appliance to send messages to a syslog server:

1. From the Grid tab, select the Grid Manager tab -> Members tab, and then click Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the Monitoring tab, and then complete the following:
   - **Syslog**: In addition to storing the syslog on a Grid member, you can configure the Grid to send the log to an external syslog server.
     - **Syslog size (MB)**: Specify the maximum size for a syslog file. Enter a value between 10 and 300. The default is 300. When the syslog file reaches the size you enter here, the appliance automatically writes the file into a new file by adding a .0 extension to the first file and incrementing subsequent file extensions by 1.
     - **Log to External Syslog Servers**: Select this to enable the appliance to send messages to a specified syslog server. Grid Manager displays the current syslog servers in the table. To define a new syslog server, click the Add icon and complete the following:
       - **Address**: Enter the IP address of the syslog server. Entries may be an IPv4 or IPv6 address.
       - **Transport**: From the drop-down list, select whether the appliance uses Secure TCP, TCP or UDP to connect to the external syslog server.
       - **Server Certificate**: Click Select to upload a self-signed or a CA-signed server certificate. In the Upload dialog, click Select and navigate to the certificate file, and then click Upload. Note that this is valid only for Secure TCP transport.
       - **Interface**: From the drop-down list, select the interface through which the appliance sends syslog messages to the syslog server:
         - **Any**: The appliance chooses any port that is available for sending syslog messages.
         - **LAN**: The appliance uses the LAN1 port to send syslog messages.
         - **MGMT**: The appliance uses the MGMT port if it has been configured. Otherwise, it uses the LAN1 port.
       - **Source**: From the drop-down list, select which syslog messages the appliance sends to the external syslog server:
         - **Any**: The appliance sends both internal and external syslog messages.
         - **Internal**: The appliance sends syslog messages that it generates.
         - **External**: The appliance sends syslog messages that it receives from other devices, such as syslog servers and routers.
       - **Node ID**: Specify the host or node identification string that identifies the appliance from which syslog messages are originated. This string appears in the header message of the syslog packet. Select one of the following:
         - **LAN**: Use the LAN1 IP address of the appliance. For an HA pair, this is the LAN1 address of the active or passive node. This is the default.
         - **Manager Name**: Use the host name of the appliance in FQDN format.
         - **IP and Host Name**: Use both the FQDN and the IP address of the appliance. The IP address can be the LAN1 or MGMT IP address depending on whether the MGMT port has been configured. Note that if the MGMT port is
Use the MGMT IP address, if the port has been configured. If the MGMT port is not configured, the LAN1 IP address is used. This can be an IPv4 or IPv6 address.

- **Port**: Enter the destination port number. The default is 514 for TCP and UDP. For Secure TCP, the default port is 6514.
- **Severity**: Choose a severity filter from the drop-down list. When you choose a severity level, the appliance sends log messages with the selected level and the levels above it. The severity levels range from the lowest, debug, to the highest, emerg. For example, if you choose debug, the appliance sends all syslog messages to the server. If you choose err, the appliance sends messages with severity levels err, crit, alert, and emerg.
- **syslog prefixes**: Use the arrows to move logging categories from the Available table to the Selected table and vice versa. The appliance sends syslog messages for the categories that are in the Selected table. When you select this option, you must add at least one logging category. The syslog messages are prefixed with a category name to which it belongs. Also, the RPZ events logged in the syslog messages uses specific prefixes for the selected categories. Note that the syslog messages are prefixed when you select logging categories for at least one external syslog server, even if you set other external syslog servers as Send All. For information about syslog prefixes, see 4817325.

**Note**: The syslog categories you specify here are different from that of logging categories specified in the Logging tab in the Grid DNS Properties or Member DNS Properties editor. The external server preserves contents of the selected categories even when selection is changed from Send all to Send selected categories and vice versa.

- **Click Add** to add the external syslog server information.
- **Copy Audit Log Messages to Syslog**: Select this for the appliance to include audit log messages it sends to the syslog server. This function can be helpful for monitoring administrative activities on multiple appliances from a central location.
  - **Syslog Facility**: This is enabled when you select Copy audit log messages to syslog. Select the facility that determines the processes and daemons from which the log messages are generated.

3. Save the configuration and click Restart if it appears at the top of the screen.

**Syslog Message Prefixes**

You can configure the syslog external backup servers to send (archive) syslog files to different destinations by their logging categories. This allows you to split syslog files based on the service and efficiently perform troubleshooting. For example, you can archive all DNS related logs on Server 1, and all DHCP related logs on Server 2. For information about how to configure an external syslog backup server, see 4817325.

When you select the Send selected categories option, the syslog messages are prefixed with a category name to which it belongs.

For syslog message prefixes to be enabled, you must check the Log to External Syslog Servers check box in Grid Properties > Monitoring. Also, the external syslog server (which can be a virtual or a physical server) must have at least one of the syslog categories selected instead of the Send all option selected in the Logging Category field.

**Note**: When you set Send all in the Logging Category, the appliance logs syslog messages for all the events and they are not prefixed. The syslog messages are prefixed even if one external syslog server is set with the Send selected categories option.

Following are the prefixes used for different logging categories:

- **DNS Logging Categories**: All DNS related messages use the following prefixes: client, config, database, dnssec, general, lame_servers, network, notify, queries, query_rewrite, resolver, responses, rpz, security, update, update_security, xfer_in, and xfer_out.

Sample syslog message for queries:

```
2014-10-27T08:15:49+00:00 daemon ib-10-35-117-12.infoblox.com named[1923]: info queries: client 10.35.117.12#55190 (1.0.0.127.in-addr.arpa): query: 1.0.0.127.in-addr.arpa IN PTR +E (10.35.117.12)
```

Sample syslog message for xfer-out:

```
```
Note: There is no prefix for RPZ syslog messages that does not belong to the DNS or ADP category.

- **ADP**: All Infoblox related messages use prefix adp.

- **DHCP**: All DHCP related messages use the following prefixes: dhcpd, omshell, dhcrelay, and dhclient.

  Sample syslog message for dhcp:

  Sep 4 09:23:44 10.34.6.28 dhcpd[20310]: DHCPACK on 70.1.20.250 to fc:5c:fc:5f:10:85 via eth1 relay 10.120.20.66 lease-duration 600

- **DTC**: All DTC related messages use the following prefixes: idns_healthd and idnsd.

  Sample syslog message for idns_healthd:

  Sep 3 12:12:35 10.34.6.30 idns_healthd[1220]: resource health status [Monitor 'icmp' (ICMP, port 0) checked server 's1' (IP 10.34.6.23), status: IPv4=ONLINE]

- **Cloud**: All cloud related messages use prefix cloud_api.

  Sample syslog message for cloud_api:

  Sep 4 10:53:30 10.34.6.32 cloud_api[5354]: [admin]: Login_Allowed -- to=Serial040Console apparently_via=Remote ip=10.120.20.66 auth=Local group=.admin-group

- **NTP**: All NTP related messages use prefix ntpd.

  Sample syslog message for NTP:

  Sep 28 06:57:21 10.35.116.7 ntpd[12186]: precision = 0.053 usec

  Sep 28 06:57:21 10.35.116.7 ntpd[12186]: Listening on interface #0 wildcard, 0.0.0.0#123 Disabled

- **File Distribution**: All File Distribution related messages use the following prefixes: ftpd and tftp.

  Sample syslog message for TFTP:

  Sep 3 13:03:09 10.34.6.30 monitor[23623]: Type: TFTP, State: Red, Event: A TFTP daemon failure has occurred

- **Authentication**: All Authentication related messages use the following prefixes: auth, authpriv, AD, and radiusd.

  Sample syslog message for RADIUS authentication:

  Sep 28 10:09:55 10.35.116.4 httpd: 2015-09-28 10:09:55.912Z [user1]: Login_Allowed -- to=AdminConnector ip=10.120.253.227 auth=RADIUS group=admin-group apparently_via=GUI

- **Microsoft Integration**: All Microsoft Integration related messages use the following prefixes: dns_server, connect_status, dns_zone, dhcp_server, dhcp_leases, clear_lease, ad_site, and ad_users.

  Sample syslog message for microsoft integration:

  dns_server:

  Sep 7 09:46:17 10.34.22.20 mssyncd[22315]: dns_server address 10.102.30.157 : Conflict in property Forwarders: NIOS value (property=<NULL IP array>) and Microsoft value (property={10.0.2.35, 10.0.2.60}). Resolved by using the Microsoft value

  dhcp_server:

  Sep 7 10:08:48 10.34.22.20 mssyncd[22316]: dhcp_server address 10.102.30.157 : Couldn't open RPC interface <MS-WKST>: an instance of a named pipe cannot be found in the listening
IP Address Used in the Syslog Configuration File

The following table describes which IP address the appliance uses as the node ID in the syslog configuration file, provided that the MGMT port has been configured. If the MGMT port is not configured, the LAN1 IP address is always used regardless of the configuration.

Table 37.1 IP address Used in Syslog Config File when MGMT Port is Configured

<table>
<thead>
<tr>
<th>Interface</th>
<th>Node ID</th>
<th>IP used in syslog configuration file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>MGMT</td>
<td>MGMT IP address</td>
</tr>
<tr>
<td>Any</td>
<td>IP and Host Name</td>
<td>MGMT IP address</td>
</tr>
<tr>
<td>MGMT</td>
<td>MGMT</td>
<td>MGMT IP address</td>
</tr>
<tr>
<td>MGMT</td>
<td>IP and Host Name</td>
<td>MGMT IP address</td>
</tr>
<tr>
<td>LAN</td>
<td>MGMT</td>
<td>LAN1 IP address</td>
</tr>
<tr>
<td>LAN</td>
<td>IP and Host Name</td>
<td>LAN1 IP address</td>
</tr>
</tbody>
</table>

Configuring Syslog Backup Servers

You can configure external syslog backup servers to forward rotated syslog files. You can configure up to 10 external syslog backup servers. To configure external backup servers:

1. **Grid**: From the Grid tab -> Grid Manager tab, expand the Toolbar and click Grid Properties -> Edit. 
   **Member**: From the Grid tab -> Grid Manager tab, click the Members tab, select the member check box, and click the Edit icon.

2. **Grid**: In the Grid Properties editor, select the Syslog Backup tab. 
   **Member**: In the Grid Member Properties editor, select the Syslog Backup tab and then click Override to override the Grid-level settings. Complete the following to modify backup server settings:
   - **Address**: Enter the IP address of the external backup server. You are not allowed to configure more than one server using the same IP address at the same level (Grid or member). However, you can use the same server IP address at different levels (Grid or member). Note that you cannot modify the IP address for the overridden server.
   - **Protocol**: Select SCP or FTP from the drop-down list.
   - **Port**: Enter the destination port number. The default port is 20 for FTP and 22 for SCP.
   - **Path**: Enter the directory path for the syslog file.
   - **Username**: Enter the username of your FTP or SCP account.
   - **Password**: Enter the password of your FTP or SCP account. If you do not change the password of the overridden server, then make sure that you use the same password specified at the Grid level.
   - **Enabled**: Select this check box to enable the FTP or SCP server. The appliance forwards the rotated syslog files to the external servers that you configure only after you select this check box. Clear the check box to disable the server.

3. Click Save and Close.

Configuring Syslog for Grid Members

You can override Grid-level syslog settings and enable syslog proxy for individual members. When you enable syslog proxy, the member receives syslog messages from specified devices, such as syslog servers and routers, and then forwards these messages to an external syslog server. You can also enable appliances to use TCP for sending syslog messages. Using TCP is more reliable than using UDP; this reliability is important for security, accounting, and auditing messages sent through the syslog. Note that you cannot enable syslog proxy for Grid members, if they are configured on a Grid Master.

To configure syslog parameters for a member:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> member check box, and then click the Edit icon.

2. In the Grid Member Properties editor, select the Monitoring tab -> Basic tab, click Override in the Syslog section, and then complete the fields as described in 4817325.

   In addition to storing the system log on a Grid member, you can configure a member to send the log to a syslog server.

3. Select the Advanced tab and complete the following:
   - **Enable syslog proxy**: Select this to enable the appliance to receive syslog messages from other devices, such as syslog servers and routers, and then forward these messages to an external syslog server.
     - **Enable listening on TCP**: Select this if the appliance uses TCP to receive messages from other devices. Enter the number of the port through which the appliance receives syslog messages from other devices.
Enable listening on UDP: Select this if the appliance uses UDP to receive messages from other devices. Enter the number of the port through which the appliance receives syslog messages from other devices.

Proxy Access Control: Select one of the following to configure access control when receiving syslog messages from specific syslog servers or routers:

None: Select this if you do not want to configure syslog proxy. When you select this option, none of the devices can send syslog messages to the appliance. This is selected by default.

Named ACL: Select this and click Select Named ACL to select a named ACL that contains only IPv4 addresses and networks. This does not support TSIG key based ACEs. When you select this, the appliance permits clients that have low permission in the named ACL to allow syslog messages from specific syslog servers or routers. You can click Clear to remove the selected named ACL.

Set of ACLs: Select this to configure individual access control entries (ACEs). Click the Add icon and select one of the following from the drop-down list. Grid Manager adds a row to the table.

IPv4 Address or IPv6 Address: Select this to add an IPv4 or IPv6 address entry. Click the Value field and enter the address. The default permission is Allow, which means that the appliance allows access to and from this device. You can change this to Deny to block access.

IPv4 Network or IPv6 Network: Select this to add an IPv4 or IPv6 network entry. Click the Value field and enter the network. The default permission is Allow, which means that the appliance allows syslog messages sent by this network. You can change this to Deny to block access.

Any Address/Network: Select this to allow or deny access to all IPv4 and IPv6 addresses and networks. The default permission is Allow, which means that the appliance allows syslog messages sent by all addresses and networks. You can change this to Deny to block access.

After you have added access control entries, you can do the following:

Select the ACEs that you want to group and put into a named ACL. Click the Create new named ACL icon and enter a name in the Convert to Named ACL dialog box.

Reorder the list of ACEs using the up and down arrows next to the table.

Select an IPv4 network and click the Edit icon to modify the entry.

Select an ACE and click the Delete icon to delete the entry. You can select multiple ACEs for deletion.

4. Save the configuration and click Restart if it appears at the top of the screen.

Setting DNS Logging Categories

You can specify logging categories you want the syslog to capture. Furthermore, you can filter these messages by severity at the Grid and member levels. For information about severity types, see 4817325.

To specify logging categories:

1. From the Data Management tab, select the DNS tab, and then click Grid DNS Properties from the Toolbar.
   or
   From the Data Management tab, select the DNS tab -> Members tab -> Grid_member check box, and then click the Edit icon.
2. In the Grid DNS Properties or Member DNS Properties editor, click Toggle Expert Mode if the editor is in the basic mode, select the Logging tab, and then complete the following:

Logging Facility: Select a facility from the drop-down list. This is the location on the syslog server to which you want to sort the DNS logging messages.

Logging Category: Select one or more of these log categories:

   - general: Records the BIND messages that are not specifically classified.
   - client: Enables the logging of messages related to query processing, but not the queries themselves. Examples of messages include exceeding recursive client quota, and other errors related to recursive clients, blacklist and NXDOMAIN interception, query name rewrite, and others.
   - config: Records the configuration file parsing messages.
   - database: Records BIND’s internal database processes.
   - dnssec: Records the DNSSEC-signed responses.
   - lame servers: Records bad delegation instances.
   - network: Records the network operation messages.
   - notify: Records the asynchronous zone change notification messages.
   - queries: Records the DNS queries. Note that enabling the logging of queries and responses will significantly affect system performance. Ensure that your system has sufficient CPU capacity before you enable DNS query logging.
   - rate-limit: Logs RRL (Response Rate Limiting) events. You must enable RRL in order for the appliance to log RRL events to this logging category.
   - resolver: Logs messages related to outgoing queries from the ‘named’ process, when it is acting as a resolver on behalf of clients.
   - responses: Records DNS responses. Note that enabling the logging of queries and responses will significantly affect system performance. Ensure that your system has sufficient CPU capacity before you enable DNS response logging.
   - rpz: Records log messages when responses are modified through RPZs or for which explicit passthru were invoked in the RPZs. This check box is not selected by default.
   - security: Logs miscellaneous messages that are related to security, such as denial or approval (mostly denial) of certain operations.
   - transfer-in: Records zone transfer messages from the remote name servers to the appliance.
   - transfer-out: Records zone transfer messages from the NIOS appliance to remote name servers.

Copyright ©2019, Infoblox, Inc. All right reserved.
• **update**: Records the dynamic update instances.
• **update-security**: Records the security updates.
• **DTC load balancing**: Records information about which client is directed to which server.
• **DTC health monitors**: Records any changes to the health state of a monitored server.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

### Viewing the Syslog

1. From the **Administration** tab, select the **Logs** tab -> **Syslog** tab.
2. From the drop-down list at the upper right corner, select the Grid member on which you want to view the syslog.
3. Optionally, use the filters to narrow down the system messages you want to view. Click **Show Filters** to enable the filters. Configure the filter criteria, and then click **Apply**.

   Based on your filter criteria (if any), Grid Manager displays the following in the **Syslog** viewer:

   - **Action icon**: The Action icon column is displayed only when you have installed the RPZ license. Click this to view threat details in the **RPZ Threat Details** dialog box. For information, see [4817325](4817325)
   - **Timestamp**: The date, time, and time zone of the log message. The time zone is the time zone configured on the member.
   - **Facility**: The location on the syslog server that determines the processes and daemons from which the log messages are generated.
   - **Level**: The severity of the message. This can be ALERT, CRITICAL, DEBUG, EMERGENCY, ERROR, INFO, NOTICE, or WARNING.
   - **Server**: The name of the server that logs this message, plus the process ID.
   - **Message**: Detailed information about the task performed. For Cloud Network Automation, this contains comma separated values of the admin, source, action, object, object type and message values. Note that source is defined only if the cloud API request was proxied by the Cloud Platform Appliance. The format for this field is **proxied from:host,IP** where **host** and **IP** are the host name and IP address of the proxy.

**Note**: If the selected member is an HA pair, Grid Manager displays the syslog in two tabs — **Active** and **Passive**.

Click the corresponding tab to view the syslog for each node.

### Viewing the RPZ Threat Details

Make sure that DNS resolution is enabled and running properly on the member to view threat details. To view threat details for the RPZ zones being queried, complete the following:

1. From the **Administration** tab, select the **Logs** tab -> **Syslog** tab.
2. Click the Action icon

   and select **View Threat Context** to open the **RPZ Threat Details** dialog. The **View Threat Context** option is disabled if there is no RPZ rule.

   - **RPZ Rule**: Displays the name of the RPZ rule.
   - **First Identified**: The date and timestamp of the first occasion that the threat was detected.
   - **Short Description**: The brief description of the threat.
   - **Description**: The description of the RPZ rule.

**Note**: The **RPZ Threat Details** dialog box may display **Unknown** if threat is unknown or **Unavailable** if threat is known and threat details are not available.

3. Click the Close icon to close the **RPZ Threat Details** dialog.

You can also do the following in the **Syslog** viewer:

- Toggle between the single line view and the multi-line view for display.
- Navigate to the next or last page of the file using the paging buttons.
- Refresh the syslog output with newly logged messages.
- Click the Follow icon to have the appliance automatically refresh the log every five seconds.
- Clear the contents of the syslog.
- Use filters and the **Go To** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- To filter Microsoft synchronization related events, click **Show Filter**, select **Server** from the first drop-down list, and select **MS_Server** from the drop-down list in the value field. This filter displays entries that begin with the prefix **ms**. To view values that belong to a specific
Microsoft server, you must specify either the name or IP address of a given Microsoft server in the Message field. When you filter the syslog for a specific Grid member, it displays the log entries of Microsoft servers that are assigned to the respective Grid member when the entries are logged.

- Print the report or export it in CSV format.
- Bookmark the syslog page.

Searching in the Syslog

Instead of paging through the syslog to locate messages, you can have the appliance search for syslog messages with certain text strings. To search for specific messages:

- Enter a search value in the search field below the filters, and then click the Search icon.
  The appliance searches through the syslog and highlights the search value in the viewer. You can use the arrow keys next to the Search icon to locate the previous or next message that contains the search value.

Downloading the Syslog File

You can download the syslog file to a specified directory, if you want to analyze it later.

1. From the Administration tab, select the Logs tab -> Syslog tab, and then click the Download icon.
2. Navigate to a directory where you want to save the file, optionally change the file name (the default names are node_1_sysLog.tar.gz and node_2_sysLog.tar.gz), and then click OK. If you want to download multiple syslog files to the same location, rename each downloaded file before downloading the next.

**Note:** If your browser has a pop-up blocker enabled, you must turn off the pop-up blocker or configure your browser to allow pop-ups for downloading files.

Viewing the Grid Node Tree

You can view graphical representation of the Grid, with its members represented as nodes in the tree. The Visualization tab is disabled for new installations and this tab is displayed by default when you upgrade to NIOS 7.2.x and later. For information about enabling this option, see Enabling Grid Visualization. Each member is labeled with its hostname. You can click Display Node Labels on the left panel to display or hide the labels.

By default, the Grid Master is the root node at the center of the tree. It is represented by a color-coded icon connected to its members. You can then click a member to re-center the tree on that node. The left panel displays information about the member that is at the center of the node tree.

In the node tree, the shape of the icons indicate the role of the member in the Grid:

- Circle: Grid Master
- Ellipse: Grid Members

The colors of the icons indicate the status of the member:

- Green: The member is online and functioning properly.
- Grey: The member has not joined the Grid.
- Red: The member has operational problems.

The connectors indicate the connection status between the Grid Master and the member.

- Blue Line: Connects the Grid Master with online Grid members
- Thick White Line: Connects the Grid Master with Grid Master Candidates
- Dashed Line Connector: Connects the Grid Master with offline Grid members

The node tree includes zooming and panning capabilities to enable quick navigation and selection among multiple nodes. You can also hover your mouse over a node to view node information. It displays the same information as that displayed on the left panel, when a node is at the center of the tree.

For the Grid Master:

- Grid name
- Standalone or HA
- Number of members in the Grid
- Status of each protocol running on the Grid
- Grid status For a Member:
  - Member name
  - Standalone or HA
  - HA Status if HA pair
  - Status of each protocol running on that member
Chapter 38 DHCP Fingerprint Detection

This chapter explains the Infoblox DHCP fingerprint detection feature and how to configure it on the appliance. It also explains how to configure DHCP fingerprints for IPv4 and IPv6.

It contains the following sections:

- Infoblox DHCP Fingerprint Detection
  - About DHCP Fingerprints
  - Standard and Custom DHCP Fingerprints
  - Administrative Permissions
- Enabling and Disabling DHCP Fingerprint Detection
- Configuring DHCP Fingerprints
  - Adding New DHCP Fingerprints
  - Modifying Custom DHCP Fingerprints
  - Deleting Custom DHCP Fingerprints
  - Viewing DHCP Fingerprint Information

Infoblox DHCP Fingerprint Detection

The NIOS appliance utilizes DHCP fingerprint detection to identify IPv4 and IPv6 mobile devices such as laptop computers, tablets and smart phones, on your network. Due to the broadcast and pervasive nature of DHCP, using DHCP fingerprint detection is an efficient way to perform system identification and inventory. You can use DHCP fingerprint detection to track devices on your network, block those that are not allowed (such as gaming consoles and home routers), and plan for future growth by accessing trending information such as the number of Apple iPhones versus that of Android phones.

When a remote DHCP client sends a DHCP REQUEST message, it includes a set of DHCP options, such as option 55 and 60. Option 55 contains an option number sequence the appliance uses to interpret the list of DHCP options that the client requests. The appliance returns the values of these requested options if the information is available.

Option 60 contains a value that indicates the device type of the requesting client. Information in option 55 or 60 is incorporated to form a unique identifier known as the DHCP fingerprint, which the appliance uses to identify the requesting client.

On an Infoblox appliance, DHCP fingerprint detection is enabled by default for all new installations. You can disable this feature at the Grid and member levels. For information, see Enabling and Disabling DHCP Fingerprint Detection. As illustrated in Figure 38.1, the appliance automatically matches option 55 and then option 60 in DHCP REQUEST messages against standard and custom DHCP fingerprints in the database. Once the appliance finds a match, it either grants or denies a lease to the requesting client based on the DHCP fingerprint filters that you apply to the DHCP range.

For information about how to configure DHCP fingerprints, see Configuring DHCP Fingerprints. For information about how to define and apply DHCP fingerprint filters, see Defining DHCP Fingerprint Filters and Applying Filters to DHCP Objects. To obtain trending information about the top OSs (operating systems) or vendor IDs for remote clients, Infoblox provides a few reports from which you can extract data. For information about reports, see Infoblox Reporting and Analytics.

Figure 38.1 DHCP Fingerprint Detection

A remote client requests a lease. Its vendor ID matches the DHCP fingerprint of a gaming console. Based on the DHCP fingerprint filter criteria, the appliance denies a lease to the requesting client.

A remote client requests a lease. Its option number sequence matches the DHCP fingerprint of an Android phone. Based on the DHCP fingerprint filter criteria, the appliance grants a lease to the requesting client.

About DHCP Fingerprints

The reporting server collects data about the remote clients and generates reports you can use to monitor the devices.
When a DHCP client sends a REQUEST message and includes DHCP option 55 (the parameter request list) and option 60 (the vendor identifier), it provides information about its OS and device type. The combination of the option sequence or vendor ID in option 55 or 60 is used to infer the OS and device type of the remote client. These parameters are then incorporated into a DHCP fingerprint that provides unique information about this client.

For example, the option number sequence for a Microsoft Windows XP system in option 55 can be one of the following:

- 1,15,3,6,44,46,47,31,33,249,43
- 1,15,3,6,44,46,47,31,33,249,43,252
- 1,15,3,6,44,46,47,31,33,249,43,252,12
- 15,3,6,44,46,47,31,33,249,43
- 15,3,6,44,46,47,31,33,249,43,252
- 28,2,3,15,6,12,44,47

The option number sequence for an Apple iPhone can be one of the following:

- 1,3,6,15,119,78,79,95,252
- 1,3,6,15,119,95,252,44,46,47

In addition, DHCP option 60 tracks vendor ID. This information can be very generic or quite specific. For example, the vendor ID MSFT 5.0 for a Microsoft Windows XP system and a Windows Vista system can be the same. For certain Cisco VoIP devices, the vendor ID can be Cisco Systems, Inc. IP Phone, which is very generic; or it can be Cisco Systems, Inc. IP Phone 7912, which is more specific. Depending on how specific the option number sequence and the vendor ID are, this information can form a unique identifier, the DHCP fingerprint, for a remote client.

**Note:** If you have enabled firewall, and if the corresponding firewall rules or policies are set to modify options 55 and 60 of the remote DHCP client to mask the identity of the client, then NIOS fingerprinting will not be able to fingerprint the clients.

### Configuring DHCP Fingerprints

The appliance installs standard DHCP fingerprints when you first install or upgrade to NIOS 6.7 and later. You cannot modify standard DHCP fingerprints nor delete them, but you can disable them. When you disable a DHCP fingerprint, the appliance disables the associated option number sequence and vendor ID, and it cannot match a remote device against the disabled DHCP fingerprint.

When you add a new DHCP fingerprint, the appliance marks it as a custom DHCP fingerprint. For information about adding custom DHCP fingerprints, see Adding New DHCP Fingerprints. You can modify information about custom DHCP fingerprints, and you can delete them. For information, see Modifying Custom DHCP Fingerprints and Deleting Custom DHCP Fingerprints. When you delete a custom DHCP fingerprint, the appliance moves it to the Recycle Bin, if enabled. You can later restore it from the Recycle Bin if needed.

Activities, such as additions, modifications, and deletions of DHCP fingerprints, are recorded in the audit log. For information about how to use the audit log, see Using the Audit Log.

**Note:** The appliance periodically updates the cached DHCP fingerprints. When you add, modify, or delete a DHCP fingerprint, you do not need to restart services but it may take up to two minutes before the appliance updates the DHCP fingerprint.

### Adding New DHCP Fingerprints

To add a custom DHCP fingerprint:

1. From the Data Management tab, select the DHCP tab -> Fingerprint tab, and then click the Add icon.
2. In the Add DHCP Fingerprint wizard, complete the following:
   - **Device Class:** From the drop-down list, select the device category to which this new fingerprint belongs. You can also enter a new device class here. When you enter a device class that already exists, the appliance matches the entry and uses the class from the current list. Device class is used for filtering purposes. For information about DHCP fingerprint filters, see Defining DHCP Finger Filters.
   - **Vendor Identifier:** Click the Add icon in the table. The appliance adds a row to the table. Click the row and enter the DHCP option number you want the appliance to validate. Valid values are from 0 to 255. When you enter more than one option, you must use commas (without spaces) to separate the numbers. For example, you can enter 1,15,3,6,44,46,47,31,33 for a Windows XP system.
   - **Option Number Sequence:** Click the Add icon in the table. The appliance adds a row to the table. Click the row and enter a Windows XP system. You can also select an option sequence and click the Delete icon to delete it. Note that if you enter an option sequence that already exists in a standard DHCP fingerprint, you must disable that standard fingerprint before you can add the option sequence to the new DHCP fingerprint.
   - **Disabled:** Select this if you want to save the configuration for the DHCP fingerprint but do not want to activate it yet. You can clear this check box when you are ready to use this DHCP fingerprint.
   - **Comment:** Enter additional information about the custom DHCP fingerprint.

3. Save the configuration or click Next to define extensible attributes. For information, see Using Extensible Attributes.
To schedule this task, click the Schedule icon at the top of the wizard. In the Schedule Change panel, click Later, and then specify a date, time, and time zone.

Modifying Custom DHCP Fingerprints

You can modify custom DHCP fingerprints, but not standard ones. Note that the appliance periodically updates the cached DHCP fingerprints. When you modify a DHCP fingerprint, you do not need to restart services but it may take up to two minutes before the appliance updates the DHCP fingerprint.

To modify a custom DHCP fingerprint:

1. From the Data Management tab, select the DHCP tab -> Fingerprint tab -> custom_fingerprint check box, and then click the Edit icon.
2. The DHCP Fingerprint editor provides the following tabs from which you can modify information:
   - **General**: Modify general information, such as the name and device class, as described in Adding New DHCP Fingerprints. Note that when you change the name of a DHCP fingerprint, the old name no longer exists, and you cannot use it for searching or filtering purposes. You may not be able to modify all fields in a standard DHCP fingerprint.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with the DHCP fingerprint. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes. Note that you cannot modify extensible attributes for standard fingerprints.
3. Save the configuration.

To schedule this task, click the Schedule icon at the top of the wizard. In the Schedule Change panel, click Later, and then specify a date, time, and time zone.

Deleting Custom DHCP Fingerprints

When you delete a custom DHCP fingerprint, the appliance moves it to the Recycle Bin, if enabled. You can later restore the DHCP fingerprint if needed. Note that you cannot delete standard DHCP fingerprints.

To delete a custom DHCP fingerprint:

1. From the Data Management tab, select the DHCP tab -> Fingerprint tab -> custom_fingerprint check box, and then click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes to delete the DHCP fingerprint.

To schedule this task, click the Delete icon -> Schedule Delete. In the Schedule Deletion dialog box, click Delete Later, and then specify a date, time, and time zone.

Viewing DHCP Fingerprint Information

The following are a few ways you can view DHCP fingerprint information:

- In a Grid with a reporting server, you can view reports that contain information about the top OSs and device types of the leasing clients in your network. For more information, see DHCP Dashboards.
- The appliance provides a few predefined smart folders from which you can view lease information about specific device groups, such as gaming consoles and Microsoft Windows devices. For more information, see Predefined Smart Folders.
- When the appliance finds a DHCP fingerprint match for a client, Grid Manager displays either the fingerprint name or the vendor ID in the following panels of Grid Manager: IP List, Current Lease, Lease History, and DHCP Range panels. You can see this information in the Fingerprints column in these panels.
- The appliance records all DHCP fingerprint related activities in the audit log. For more information, see Using the Audit Log.

Enabling and Disabling DHCP Fingerprint Detection

Grid DHCP fingerprint detection is enabled by default for new installations, and no special licenses are required. You can disable this or override the Grid setting at a member level. Note that when you enable DHCP fingerprint detection, there will be a slight impact on DHCP performance.

When you enable DHCP fingerprint on an HA pair, both peers in a failover association maintain the same DHCP fingerprinting state (enabled or disabled) even when one of the peers fails or becomes operational again. Note that both peers must be in the same Grid for the fingerprinting state to stay the same. For information about DHCP failover, see About DHCP Failover.

To enable and disable Grid DHCP fingerprinting:

1. **Grid**: From the Data Management tab, select the DHCP tab, and then click Grid DHCP Properties from the Toolbar.
   - **Member**: From the Data Management tab, select the DHCP tab -> Members tab -> Members -> member check box, and then click the Edit icon.
2. In the Grid DHCP Properties or Member DHCP Properties editor, select the Fingerprinting tab.
3. Complete the following:
   - **Enable Fingerprint Detection**: Deselect this check box to disable the feature. You can enable DHCP fingerprint detection again by selecting the check box. Click Override to change the configuration for a member, or click Inherit to inherit the Grid setting.
Standard and Custom DHCP Fingerprints

Standard DHCP fingerprints are automatically installed on the appliance when you first set it up or after you have completed an upgrade from previous NIOS releases to NIOS 6.7 and later. Note that new DHCP fingerprints are added to the appliance during a major NIOS upgrade. For more information about upgrades, see About Upgrades.

Note: When you upgrade to NIOS 6.7 and later, DHCP fingerprint detection is disabled during the upgrade. You must enable it if you want the appliance to use DHCP fingerprint detection. For information, see Enabling and Disabling DHCP Fingerprint Detection.

You can configure custom DHCP fingerprints for devices whose DHCP fingerprints are not captured in the standard DHCP fingerprints. For information about how to add custom DHCP fingerprints, see Adding New DHCP Fingerprints.

Both standard and custom DHCP fingerprints are cached in memory for matching purposes. Depending on the information provided in a DHCP fingerprint, the appliance first matches the option number sequence sent in the DHCP REQUEST message. If option 55 is not included in the request or if there is no match from the cached DHCP fingerprints, the appliance then tries to match the vendor ID in option 60. When there is an option number sequence match, the appliance displays the name of the DHCP fingerprint in Grid Manager. If there is no option number sequence match but there is a vendor ID match, the appliance displays the vendor ID. For information about how to view fingerprint information, see Viewing DHCP Fingerprint Information.

You can also create IPv4 and IPv6 DHCP fingerprint filters and then apply them as class filters to specific IPv4 and IPv6 DHCP ranges and range templates. For information about how to configure and use DHCP fingerprint filters, see About DHCP Fingerprint Filters.

Chapter 39 Monitoring with SNMP

This chapter describes how you can use SNMP (Simple Network Management Protocol) to monitor NIOS appliances in your network. It contains the following sections:

- Understanding SNMP
  - About SNMPv1 and SNMPv2
  - About User-Based Security Model in SNMPv3
- Configuring SNMP
  - Configuring SNMPv3 Users
  - Modifying SNMPv3 Users
  - Deleting SNMPv3 Users
  - Accepting Queries
  - Adding Trap Receivers
  - Defining Thresholds for Traps
  - Setting SNMP and Email Notifications
  - Setting SNMP System Information
  - Testing the SNMP Configuration
- SNMP MIB Hierarchy
  - MIB Objects
  - System Object IDs
- Infoblox MIBs
  - Loading the Infoblox MIBs
  - ibTrap MIB
  - ibPlatformOne MIB
  - ibDHCPOne MIB
  - ibDNSOne MIB
  - IB-DNSSERV-MIB
  - IB-DNSHITRATIO-MIB
  - IB-DNSQUERYRATE-MIB
  - IB-DHCPSErv-MIB

Understanding SNMP

You can use SNMP (Simple Network Management Protocol) to manage network devices and monitor their processes. An SNMP-managed device, such as a NIOS appliance, has an SNMP agent that collects data and stores them as objects in MIBs (Management Information Bases). The SNMP agent can also send traps (or notifications) to alert you when certain events occur within the appliance or on the network. You can
view data in the SNMP MIBs and receive SNMP traps on a management system running an SNMP management application, such as HP OpenView, IBM Tivoli NetView, or any of the freely available or commercial SNMP management applications on the Internet.

Figure 39.1 SNMP Overview

The NIOS appliance supports SNMPv1, SNMPv2, and SNMPv3. It also adheres to the following RFCs:

- RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413, Simple Network Management Protocol (SNMP) Applications
- RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP)
- RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 1155, Structure and identification of Management information for TCP/IP-based internets
- RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II
- RFC 2578, Structure of Management Information Version 2 (SMIv2)

About SNMPv1 and SNMPv2

SNMPv1 is the initial implementation of SNMP. It operates over protocols such as UDP (User Datagram Protocol) and IP (Internet Protocol). SNMPv2 includes improvements in performance and security. It adds new protocol operations such as GetBulk and Inform, which allow the management system to request larger blocks of data from the agent. Both SNMPv1 and SNMPv2 use common strings that are sent in clear text to authenticate clients.

The NIOS appliance supports SNMPv1 and SNMPv2 in which the SNMPv2 agent acts as a proxy agent for the SNMPv1 management systems. When an SNMPv1 management system sends a query to the appliance, the SNMPv2 proxy agent forwards the request to the SNMPv1 agent. The proxy agent maps the SNMPv1 trap messages to the SNMPv2 trap messages, and then forward the messages to the management system. You can enable the appliance to receive queries from SNMPv1 and SNMPv2 management systems. You can also add SNMPv1 and SNMPv2 management systems to receive traps from the appliance. For information about how to configure SNMPv1 and SNMPv2 on the appliance, see Configuring SNMP.

About User-Based Security Model in SNMPv3

SNMPv3 adds security and remote configuration enhancements to SNMPv1 and SNMPv2. The NIOS appliance supports the USM (User-based Security Model) in SNMPv3 for the authentication, encryption, and decryption of SNMP data. SNMPv3 uses the same MIB objects as those supported in SNMPv1 and SNMPv2.

SNMPv3 provides the following security measures:

- Data integrity: Ensure that SNMP data is not maliciously modified by unauthorized entities during its transmission through the network. This protects against unauthorized management operations, such as falsifying the value of a MIB object.
- Authentication: Verify the identities of the origin of the SNMP data to protect against masquerade threats that may temper the identity of users who have the appropriate authorization to send and receive SNMP data.
Confidentiality: Ensure that unauthorized users cannot eavesdrop on any data exchanges between SNMP agents and management systems, depending on local policies of the systems.
Timeliness: Ensure that the SNMP data is received in a timely manner to prevent malicious reordering of data by unauthorized entities.

To enable SNMPv3 on the NIOS appliance to provide user-based security, you must first configure SNMPv3 users on the appliance to enable access by SNMP management systems. The appliance supports HMAC-MD5-96 and HMAC-SHA-96 hash functions as the authentication protocols, and DES (Data Encryption Standard) and AES (Advanced Encryption Standard) as the encryption methods for SNMPv3 users. For information, see Configuring SNMP.

**Configuring SNMP**

**Note:** SNMP operation is not supported across the NIOS appliance's LAN2 interface.

You can configure the appliance to receive SNMP queries from specific management systems and send SNMP traps to specific trap receivers. SNMP operation supports both IPv4 and IPv6 networks. The appliance supports SNMPv1, SNMPv2, and SNMPv3. You can set up either SNMPv1/SNMPv2 or SNMPv3, or all of them for the Grid. You can also override the Grid settings at a member level.

To configure SNMPv1 and SNMPv2 on the appliance, do the following:

- Enable the NIOS appliance to accept queries, as described in Accepting Queries.
- Specify the management systems to which the appliance sends traps, as described in Adding Trap Receivers.
- Specify system information using managed objects in MIB-II, the standard MIB defined in RFC 1213. For information, see Setting SNMP System Information.

To configure SNMPv3 on the appliance, do the following:

- Add an SNMPv3 user and set up authentication and privacy protocols. For information, see Configuring SNMPv3 Users. After you set up an SNMPv3 user, you can modify and delete it. For information, see Modifying SNMPv3 Users and Deleting SNMPv3 Users.
- Specify system information using managed objects in MIB-II, the standard MIB defined in RFC 1213. For information, see Setting SNMP System Information.

**Configuring SNMPv3 Users**

To enable SNMPv3, you must first configure SNMPv3 users on the appliance. For information about SNMPv3, see About User-Based Security Model in SNMPv3. To configure an SNMPv3 user:

1. From the Administration tab, select the SNMPv3 Users tab, and then click the Add icon.
2. In the Add SNMPv3 User wizard, complete the following:
   - **Name:** Enter a user name for the SNMPv3 management system.
   - **Authentication Protocol:** Select one of the following:
     - MD5: Select this to use the HMAC-MD5-96 authentication protocol to authenticate the SNMPv3 user. This protocol uses the MD5 (Message-Digest algorithm 5) hash function in HMAC (Hash-based Message Authentication Code) and truncates the output to 96 bits. The output is included as part of the SNMP message sent to the receiver. For detailed information about the protocol, refer to RFC 1321, The MD5 Message-Digest Algorithm.
     - SHA: Select this to use the HMAC-SHA-96 authentication protocol to authenticate the SNMPv3 user. This protocol uses the SHA (Secure Hash Algorithm) hash function in HMAC and truncates the output to 96 bits. The output is included as part of the SNMP message sent to the receiver.
     - None: Select this to decline using any authentication protocol for this SNMPv3 user. When you select this option, you are not required to enter a password.
   - **Password:** Enter a password for the selected authentication protocol.
   - **Confirm Password:** Enter the same password.
   - **Privacy Protocol:** Select one of the following:
     - DES: Select this to use DES for data encryption. DES is a block cipher that employs a 56-bit key size and 64-bit block size in the encryption.
     - AES: Select this to use AES for data encryption. AES is a symmetric-key encryption standard that comprises three block ciphers, AES-128, AES-192, and AES-256. Each of these ciphers has a 128-bit block size and a key size of 128, 192, and 256 bits, respectively.
     - None: Select this to decline using any privacy protocol for this SNMPv3 user. When you select this option, you are not required to enter a password.
   - **Password:** Enter a password for the privacy protocol.
   - **Confirm Password:** Enter the same password.
   - **Comment:** Enter useful information about the SNMP user, such as location or department.
   - **Disable:** Select this check box to retain an inactive profile for this SNMP user in the configuration. You can clear this check box to activate the profile.

**Note:** If an SNMPv3 user is configured to send SNMP queries, you cannot delete the user.

3. Click **Next** to define extensible attributes. For information, see Using Extensible Attributes.
4. Save the configuration.

Modifying SNMPv3 Users

1. From the Administration tab, select the SNMPv3 Users tab -> snmpv3user, and then click the Edit icon.
2. The SNMPv3 User editor provides the following tabs from which you can edit data:
   - **General**: Modify the data as described in Configuring SNMPv3 Users.
   - **Extensible Attributes**: Add and delete extensible attributes that are associated with the SNMPv3 user account. You can also modify the values of extensible attributes. For information, see Using Extensible Attributes.
3. Save the configuration.

Deleting SNMPv3 Users

When you delete an SNMPv3 user that is configured to send queries or receive traps, a warning message states that the SNMPv3 is associated with the corresponding function. You can then decide whether you want to delete the user or not.

To delete an SNMPv3 user:

1. From the Administration tab, select the SNMPv3 Users tab -> snmpv3user, and then click the Delete icon.
2. In the **Delete confirmation** dialog box, click Yes.

**Note**: You cannot schedule the deletion of an SNMPv3 user.

Accepting Queries

You can allow specific management systems to send SNMP queries to a NIOS appliance. For SNMPv1 and SNMPv2, you must specify a community string. The appliance accepts queries only from management systems that provide the correct community string. You can also specify SNMPv3 users to send queries. For information about configuring SNMPv3 users, see Configuring SNMPv3 Users.

To configure an appliance to accept SNMP queries:

1. Grid: From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar. Member: From the Grid tab, select the Grid Manager -> Members tab -> member, and then click the Edit icon.
2. In the Grid Properties or Grid Member Properties editor, select the SNMP tab. To override Grid settings, click **Override** in the Grid Member Properties editor.
3. Complete the following in the **SNMP** section.
   - **Enable SNMPv1/SNMPv2 Queries**: Select this to accept SNMPv1 and SNMPv2 queries from management systems.
     - **Community String**: Enter a text string that the management system must send together with its queries to the appliance. A community string is similar to a password in that the appliance accepts queries only from management systems that send the correct community string. Note that this community string must match exactly what you enter in the management system.
   - **Engine ID**: Displays the engine ID of the appliance that manages the SNMP agent. The management system needs this ID to send traps to the appliance. If the appliance is an HA pair, this field displays the engine IDs for both the active and passive nodes.
   - **Enable SNMPv3 Queries**: Select this to enable queries from SNMPv3 management systems. Click the Add icon to add SNMPv3 users that you have configured on the appliance. In the SNMPv3 User Selector dialog box, click the SNMPv3 user you want to add. The appliance displays the selected SNMPv3 users in the table. You can add comments in the table. You can also select an SNMPv3 user and click the Delete icon to remove it from the table. Note that a disabled SNMPv3 user cannot send queries to the appliance.
4. Save the configuration.

Adding Trap Receivers

You can enable the NIOS appliance to send traps to specific management systems using either SNMPv1/SNMPv2 or SNMPv3, or all versions of SNMP. You can then add management systems that are allowed to receive traps from the appliance. Note that you cannot enable both SNMPv1/SNMPv2 and SNMPv3 on the same trap receiver. The appliance sends traps when certain events occur. You can enable SNMP traps and add trap receivers to the Grid. You can also override the Grid settings at the member level.

To enable the appliance to send traps and to add trap receivers, do the following:

1. Grid: From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar. Member: From the Grid tab, select the Grid Manager -> Members tab -> member, and then click the Edit icon.
2. In the Grid Properties or Grid Member Properties editor, select the SNMP tab. To override Grid settings, click **Override** in the Grid Member Properties editor.
3. Complete the following in the **SNMP** tab:
   - **Enable SNMPv1/SNMPv2 Traps**: Select this to enable the appliance to send traps to specified management systems.
     - **Community String**: Enter a text string that the NIOS appliance sends to the management system together with its
traps. Note that this community string must match exactly what you enter in the management system.

- **Enable SNMPv3 Traps**: Select this to enable the appliance to send traps to specified SNMPv3 users.

4. Click the Add icon and select one of the following from the drop-down menu to add an SNMP trap receiver:

- **SNMPv1/SNMPv2**: Select this to add an SNMPv1 or SNMPv2 management system as a trap receiver. Grid Manager adds a row to the table. In the **Address** field, enter the IP address of the SNMP management system to which you want the SNMP agent on the appliance to send traps. You can enter more than one trap receiver. To remove a trap receiver from the list, select the address, and then click the Delete icon.

- **SNMPv3**: Select this to add an SNMPv3 management system as a trap receiver. Grid Manager displays the **SNMPv3 User Selector** dialog box. Click the name of the SNMPv3 user in the dialog box. Grid Manager adds the user to the table. In the **Address** field, enter the IP address of the SNMP management system to which you want the SNMP agent on the appliance to send traps. You can add more than one trap receiver. To remove a trap receiver from the list, select the address, and then click the Delete icon.

   Trap receiver IP addresses may be in IPv4 or IPv6 format.

   In the Trap Receiver table, Grid Manager displays the following information about the trap receivers:

   - **Address**: The IPv4 or IPv6 address of the trap receiver. Note that when an SNMPv3 user is disabled, SNMPv1/SNMPv2 traps are disabled. You can modify the IP address of the trap receiver even when the following are disabled: SNMPv3 users, SNMPv1/SNMPv2 traps, and SNMPv3 traps.
   - **SNMPv3 User**: The user name of the SNMPv3 trap receiver. This is for SNMPv3 only.
   - **Comment**: Information you entered about the management system.

5. Save the configuration.

**Setting SNMP System Information**

You can enter values for certain managed objects in MIB-II, the standard MIB defined in RFC 1213. Management systems that are allowed to send queries to the appliance can query these values. You can enter these values for the Grid and specific members. You can also override the Grid values at a member level.

To enter system information:

1. Grid: From the **Grid** tab, select the **Grid Manager** tab, and then select **Grid Properties -> Edit** from the Toolbar. Member: From the **Grid** tab, select the **Grid Manager -> Members tab -> member**, and then click the **Edit** icon.

2. In the **Grid Properties or Grid Member Properties** editor, select the **SNMP** tab. To override Grid settings, click **Override** in the **Grid Member Properties editor**.

3. Complete the following in the **SNMP** tab. For an HA member, click **Override Node 2 settings** to enter information for node 2 of the HA pair.

   - **sysContact**: Enter the name of the contact person for the appliance.
   - **sysLocation**: Enter the physical location of the appliance.
   - **sysName**: Enter the fully qualified domain name of the appliance.
   - **sysDescr**: Enter useful information about the appliance, such as the software version it is running.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

**Defining Thresholds for Traps**

Threshold events for appliance performance are configurable. For each event, you can set a value that triggers the appliance to send a trap and another value at which the appliance sends a CLEAR trap. The appliance sends a CLEAR trap the first time the event value reaches the reset value after it reached the trigger value.

To define the threshold values:

1. Grid: From the **Grid** tab, select the **Grid Manager** tab, and then select **Grid Properties -> Edit** from the Toolbar. Member: From the **Grid** tab, select the **Grid Manager -> Members tab -> member**, and then click the **Edit** icon.

2. In the **Grid Properties or Grid Member Properties** editor, click **Toggle Advanced Mode**, and then select the **SNMP Threshold** tab. To override Grid settings, click **Override** in the **Grid Member Properties editor**.

3. Complete the following in the **SNMP Threshold** tab. Each of the following event types have default Trigger and Reset values. You can change the values for any of them. You can set SNMP thresholds above or below which the appliance sends SNMP traps and email notifications, if configured to do so. When any allocated usage exceeds the Trigger value, the appliance sends an SNMP trap and email notification to the designated destination, and the status icon for that usage turns red. When usage drops to the Reset value, the status color goes back to normal and turns green.

   - **CPU Usage**: The percentage of the CPU that is currently in use. The default Trigger value is 81%, and the default Reset value is 70%. Note that these default values are set to disable the CPU usage trap. You can enable this trap and configure the trigger and reset values using the CLI command set thresholdtrap.
   - **Database Objects**: The percentage of database capacity that is currently in use. The default Trigger value is 80%, and the default Reset value is 70%.
   - **Disk**: The percentage of the primary hard disk that is currently in use. The default Trigger value is 85%, and the default Reset value is 70%.
   - **File Distribution Usage**: The percentage of the file distribution storage capacity that is currently in use on the selected member. The default Trigger value is 90%, and the default Reset value is 70%.
IPAM Utilization: For a network, this is the percentage based on the IP addresses in use divided by the total addresses in the network and for a network container that contains subnets, this is the percentage of the total address space defined within the container regardless of whether any of the IP addresses in the subnets are in use. The default Trigger value is 95% and the default Reset value is 85%. The status icon turns red when utilization crosses the configured trigger value. When utilization is below the trigger value, the status color turns blue. Memory: The percentage of the system memory that is currently in use. The default Trigger value is 90%, and the default Reset value is 80%. Network Capacity: When the Grid is part of a Master Grid, this is the percentage of the Master Grid's network capacity that is used by the Grid's networks. The default Trigger value is 85% and default Reset value is 75%. Recursive Clients: The percentage of the limit of concurrent recursive queries. The default Trigger value is 80%, and the default Reset value is 30%. You must also enable the recursive client limit in order for the appliance to send recursive client traps. For information about how to set this limit, see Restricting Recursive Client Queries. When you configure the Trigger and Reset values, ensure that you do not set them too low or too close together. If the Trigger and Reset values are too close together, the appliance may send excessive traps and email notifications because both trigger and reset traps are sent based on the calculated value of simultaneous recursive client queries. For example, when you set the recursive client limit at 50, Trigger value at 71%, and Reset value at 70%, the value for simultaneous recursive client queries is calculated at 50 x .71 = 35 (integer math truncation) and 50 x .70 = 35. This could result in the appliance sending trigger and reset traps for the same value of simultaneous recursive client queries.

Root File System: The percentage of the root file system ("/\) that is currently in use. The default Trigger value is 85%, and the default Reset value is 70%.

Swap Usage: The percentage of the swap area that is currently in use. The factory default Trigger value is 20% and the factory default Reset value is 10%. The swap usage threshold varies based on the appliance models. The Infoblox GUI displays zero for both the Trigger and Reset values indicating the optimized usage of platform specific default values. The swap usage threshold is set to 50% for 2 GB appliances and 20% for all other appliances. For information about available memory on each appliance model, see Table 39.1.

Reporting: The number of reports created on the system that can trigger an SNMP trap. The default Trigger value is 85, and the default Reset value is 70. Note that the maximum number of reports supported per Grid is 300. This field is displayed only when you have configured a reporting server.

Reporting Volume: The percentage of data transmissions to the reporting server. The default Trigger value is 80%, and the default Reset value is 71%. This field is displayed only when you have configured a reporting server.

Threat Protection Dropped Traffic: The percentage of packets dropped based on the threat protection rule configuration. The default Trigger value is 90%, and the default Reset value is 70%. This field is displayed only when Threat Protection licenses are installed on the appliance. When the percentage of Threat Protection dropped traffic exceeds the Trigger value or drops below the Reset value, the appliance sends an SNMP trap and an email notification — if configured to do so. For information about setting SNMP traps and email notifications, see Setting SNMP and Email Notifications.

Threat Protection Total Traffic: The percentage of total traffic received (dropped and passed packets) on the external interfaces. The default Trigger value is 90%, and the default Reset value is 70%. This field is displayed only when Threat Protection licenses are installed on the appliance. When the percentage of total Threat Protection traffic exceeds the Trigger value or drops below the Reset value, the appliance sends an SNMP trap and an email notification — if configured to do so. For information about setting SNMP traps and email notifications, see Setting SNMP and Email Notifications.

If you have installed Threat Protection licenses on the appliance and are using the Infoblox feature, Grid Manager displays the following for Trigger events per second and Reset events per second:

- Alert Rate: The number of SNMP traps sent per second when the appliance sends alerts while passing packets based on threat protection rule configuration. The default Trigger value is 1 and the default Reset value is 0.
- Drop Rate: The number of SNMP traps sent per second when the appliance drops packets based on the threat protection rule configuration. The default Trigger value is 1 and the default Reset value is 0.

If you have installed an RPZ license on the NIOS appliance, you can configure the thresholds to monitor the RPZ hit rate in the Response Policy Zones Hit Rate Configuration section. For information, see Configuring Thresholds for RPZ Hit Rate.

4. Save the configuration and click Restart if it appears at the top of the screen.

The following table lists available Infoblox appliance models and their available memory. Note that TE appliances are IB appliances in Grid Manager.

Table 39.1 Overview of Available Memory for Infoblox Appliance Models

<table>
<thead>
<tr>
<th>Infoblox Appliance Series</th>
<th>Appliance Model</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Platform Virtual Appliances</td>
<td>CP-V2200</td>
<td>12 GB</td>
</tr>
<tr>
<td></td>
<td>CP-V1400</td>
<td>8 GB</td>
</tr>
<tr>
<td></td>
<td>CP-V800</td>
<td>2 GB</td>
</tr>
<tr>
<td>Advanced Appliances</td>
<td>PT-4000-10GE</td>
<td>24 GB</td>
</tr>
<tr>
<td></td>
<td>PT-4000</td>
<td>24 GB</td>
</tr>
<tr>
<td></td>
<td>PT-2205-10GE</td>
<td>64 GB</td>
</tr>
</tbody>
</table>
Setting SNMP and Email Notifications

You can specify the event types that trigger trap and email notifications. To set SNMP trap and email notifications:

1. Grid: From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar. Member: From the Grid tab, select the Grid Manager -> Members tab -> member, and then click the Edit icon.

2. In the Grid Properties or Grid Member Properties editor, click Toggle Advanced Mode, and then select the Notification tab. To override Grid settings, click Override in the Grid Member Properties editor.

3. Complete the following:
   - **Enable All SNMP Notifications**: Select this check box if you want the appliance to send SNMP notifications (traps) for all events to the configured trap receivers. This is selected by default. To send SNMP notifications for specific events to the configured trap receiver, select the check box for each respective event type. For more information, see Adding Trap Receivers.
   - **Enable All Email Notifications**: Select this check box if you want the appliance to send email notifications (traps) for all events to the configured email recipients. This is deselected by default. To send email notifications for specific events to the configured email recipients, select the check box for each respective event type. For more information, see Selecting SNMP and Email Notification Types. Alternatively, you can select specific event types from the table, and specify whether you want the appliance to send SNMP
Notifications and Email notifications for each type of event.

4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Selecting SNMP and Email Notification Types

Instead of enabling and receiving SNMP and email notifications for all hardware and software events, you can select specific alert types when a specific hardware or software encounters issues. To enable SNMP or email notifications for specific event types, select the corresponding check boxes in the Notification tab of the Grid Properties or Member Properties editor. The following table lists the event types you can select:

#### Table 39.2 Event Types

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
<th>Sample SNMP Trap</th>
</tr>
</thead>
</table>
| **BGP** | Sends notifications when the BGP software has failed. For more information, see [ibProbableCause Values](#). | 2012-11-22 04:49:06
eng-lab-883.inca.infoblox.com [UDP: [10.35.3.115]:38185->[10.120.20.160]]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (45366)
0:07:33.66
SNMPv2-MIB::snmpTrapOID.0 = OID:
IB-TRAP-MIB::ibTrapOneModule.2
IB-TRAP-MIB::ibNodeName.0 = STRING: "10.35.3.115"
IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: critical(5)
IB-TRAP-MIB::ibSubsystemName.0 = STRING: bgp
IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibRevokedLicense(53)
IB-TRAP-MIB::ibTrapDesc.0 = STRING: An BGP routing daemon failure has occurred. |
| **Backup** | Sends notifications about the status of backup operation. For more information, see [Processing and Software Failure Traps](#). | 2011-09-22 09:14:17
ib-10-34-41-4.infoblox.com [UDP: [10.34.41.4]:41243->[10.34.41.4]]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (48621)
0:08:06.21
SNMPv2-MIB::snmpTrapOID.0 = OID:
IB-TRAP-MIB::ibProcessingFailureTrap
IB-TRAP-MIB::ibNodeName.0 = STRING: "10.34.41.4"
IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: minor(3)
IB-TRAP-MIB::ibSubsystemName.0 = STRING: scheduled_tftp_backups
IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibBackupSoftwareFailure(29)
IB-TRAP-MIB::ibTrapDesc.0 = STRING: Backup failed. |
| **BloxTools** | Sends notifications about the status of bloxTools. For more information, see [Object State Change Traps](#). | 2011-09-13 20:38:46
10.34.42.4 [UDP: [10.34.42.4]:38187->[10.34.42.2]]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (742156)
2:03:41.56
SNMPv2-MIB::snmpTrapOID.0 = OID:
IB-TRAP-MIB::ibStateChangeEvent
IB-TRAP-MIB::ibNodeName.0 = STRING: "10.34.42.4"
IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2)
IB-TRAP-MIB::ibObjectName.0 = STRING: bloxTools
IB-TRAP-MIB::ibPreviousState.0 = INTEGER: bloxTools-service-failed(41)
IB-TRAP-MIB::ibCurrentState.0 = INTEGER: bloxTools-service-working(39)
IB-TRAP-MIB::ibTrapDesc.0 = STRING: BloxTools Service is working. |
<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Date/Time</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Sends notifications about the status of CPU usage. For more information, see</td>
<td>2012-04-12 01:54:59</td>
<td>CPU</td>
</tr>
<tr>
<td></td>
<td><em>Threshold Crossing Traps.</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>eng-lab-631.inca.infoblox.com [UDP: [10.35.2.119]:42546-&gt;[10.120.20.160]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (786308) 2:11:03.08 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibTrapOneModule.3 IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.2.119&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: major(4) IB-TRAP-MIB::ibObjectName.0 = STRING: cpu_usage IB-TRAP-MIB::ibCurThresholdValue.0 = INTEGER: 51 IB-TRAP-MIB::ibThresholdHigh.0 = INTEGER: 5 IB-TRAP-MIB::ibThresholdLow.0 = INTEGER: 3 IB-TRAP-MIB::ibTrapDesc.0 = STRING: CPU usage above threshold value.</td>
<td></td>
</tr>
<tr>
<td>CaptivePortal</td>
<td>Sends notifications about the Captive Portal service. For more information, see ib PreviousState (OID 3.1.1.1.2.9.0) and ibCurrentState (OID 3.1.1.1.2.10.0)</td>
<td>2016-01-08 02:58:23</td>
<td>CaptivePortal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.35.107.4 [UDP: [10.35.107.4]:45111-&gt;[10.120.20.21]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (22280) 0:03:42.80 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibStateChangeEvent IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.107.4&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2) IB-TRAP-MIB::ibObjectName.0 = STRING: captive_portal IB-TRAP-MIB::ibPreviousState.0 = INTEGER: captive-portal-service-inactive(51) IB-TRAP-MIB::ibCurrentState.0 = INTEGER: captive-portal-service-working(49) IB-TRAP-MIB::ibTrapDesc.0 = STRING: Captive Portal Service is working.</td>
<td></td>
</tr>
<tr>
<td>Cisco ISE</td>
<td>Sends notifications about the status of the Cisco ISE service. For more information, see Object State Change Traps.</td>
<td>2016-01-07 22:26:19</td>
<td>Cisco ISE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.40.240.111 [UDP: [10.40.240.111]:47355-&gt;[10.120.20.21]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (16384) 0:02:43.84 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibStateChangeEvent IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.40.240.111&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2) IB-TRAP-MIB::ibObjectName.0 = STRING: cisco_ise_server IB-TRAP-MIB::ibPreviousState.0 = INTEGER: 124 IB-TRAP-MIB::ibCurrentState.0 = INTEGER: 123 IB-TRAP-MIB::ibTrapDesc.0 = STRING: CiscoISE server 10.36.141.15 is OK.</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
<td>Time</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>Clear</strong></td>
<td>Sends notifications when the SNMP trap is cleared. When you select the check box, the CLEAR trap is sent for the following software failures: LDAP servers, OCSP responders, LCD, Serial Console, OSPF, OSPF6, BGP, HSM, Controld, SSH, HTTP, Cluster, Login, and Duplicate IP. For file distribution, the trap is sent when the service is restored. If you deselect the check box, the CLEAR trap is not sent when any of the mentioned software fails. For more information, see <em>Processing and Software Failure Traps.</em></td>
<td>2015-11-12</td>
<td>22:46:21</td>
</tr>
<tr>
<td><strong>Cloud API</strong></td>
<td>Sends notifications about whether the Cloud API service is functioning or not. For information about Cloud Network Automation, see Introduction to <em>Cloud Network Automation.</em></td>
<td>2014-11-13</td>
<td>00:52:37</td>
</tr>
<tr>
<td><strong>Cluster</strong></td>
<td>Sends notifications about the status of NIOS clusterd process. For more information, see <em>Processing and Software Failure Traps.</em></td>
<td>2011-12-10</td>
<td>09:43:23</td>
</tr>
</tbody>
</table>
Controld  | Sends notifications about the NIOS controld process. For more information, see *Processing and Software Failure Traps.*
| 2012-08-17 05:29:30 |
| <UNKNOWN> [UDP: [10.32.2.80]:43475->[10.32.2.80]:162]; DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (24722) 0:04:07.22; SNMPv2-MIB::snmpTrapOID.0 = OID:
| IB-TRAP-MIB::ibProcessingFailureTrap |
| IB-TRAP-MIB::ibNodeName.0 = STRING: "192.168.1.2" |
| IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: critical(5) |
| IB-TRAP-MIB::ibSubsystemName.0 = STRING: controld |
| IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibControldSoftwareFailure(11) |
| IB-TRAP-MIB::ibTrapDesc.0 = STRING: A controld failure has occurred. |

DHCP  | Sends notifications about the status of DHCP service. For more information, see *ibPreviousState (OID 3.1.1.1.2.9.0) and ibCurrentState (OID 3.1.1.1.2.10.0).*
| 2016-04-18 02:42:36 |
| 10.35.139.15 [UDP: [10.35.139.15]:35531->[10.120.21.204]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8809) 0:01:28.09; SNMPv2-MIB::snmpTrapOID.0 = OID:
| IB-TRAP-MIB::ibStateChangeEvent |
| IB-TRAP-MIB::ibNodeName.0 = STRING: "10.35.139.15" |
| IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2) |
| IB-TRAP-MIB::ibObjectName.0 = STRING: dhcpd |
| IB-TRAP-MIB::ibPreviousState.0 = INTEGER: dhcp-service-inactive(48) |
| IB-TRAP-MIB::ibCurrentState.0 = INTEGER: dhcp-service-working(45) |
| IB-TRAP-MIB::ibTrapDesc.0 = STRING: DHCP Service is working. |

DNS  | Sends notifications about the status of DNS service. For more information, see *ibPreviousState (OID 3.1.1.1.2.9.0) and ibCurrentState (OID 3.1.1.1.2.10.0).*
| 2016-01-08 01:10:53 |
| 10.35.3.154 [UDP: [10.35.3.154]:59876->[10.120.20.12]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (324160) 0:54:01.60; SNMPv2-MIB::snmpTrapOID.0 = OID:
<p>| IB-TRAP-MIB::ibStateChangeEvent |
| IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.3.154&quot; |
| IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2) |
| IB-TRAP-MIB::ibObjectName.0 = STRING: DNS |
| IB-TRAP-MIB::ibPreviousState.0 = INTEGER: dns-service-working(32) |
| IB-TRAP-MIB::ibCurrentState.0 = INTEGER: dns-service-inactive(34) |
| IB-TRAP-MIB::ibTrapDesc.0 = STRING: DNS Service is inactive. |</p>
<table>
<thead>
<tr>
<th><strong>DNS Attack</strong></th>
<th>Sends notifications about the status of the DNS attacks. For more information, see <strong>ibPreviousState (OID 3.1.1.1.2.9.0) and ibCurrentState (OID 3.1.1.1.2.10.0)</strong>.</th>
<th>2016-01-07 23:55:56</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.35.3.201 [UDP: [10.35.3.201]:33199-&gt;[10.120.21.204]]:</td>
<td>DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (25100) 0:04:11.00</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::snmpTrapOID.0 = OID:</td>
<td>IB-TRAP-MIB::ibStateChangeEvent</td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.3.201&quot;</td>
<td>IB-TRAP-MIB::ibCurrentState.0 = INTEGER: dns-attack-inactive(116)</td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibPreviousState.0 = INTEGER: dns-attack-active(115)</td>
<td>IB-TRAP-MIB::ibObjectName.0 = STRING: DNSAttack</td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibTrapDesc.0 = STRING: DNS attack conditions have ended.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>DNS Integrity Check</strong></th>
<th>Sends notifications about whether DNS integrity check is functioning or not. For information about DNS integrity check, see <strong>About DNS Integrity Check for Authoritative Zones</strong>.</th>
<th>2014-06-03 05:35:45</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.34.82.121 [UDP: [10.34.82.121]:42577-&gt;[10.120.20.232]]:</td>
<td>DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (427200) 1:11:12.00</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::snmpTrapOID.0 = OID:</td>
<td>IB-TRAP-MIB::ibProcessingFailureTrap</td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.3.201&quot;</td>
<td>IB-TRAP-MIB::ibSubsystemName.0 = STRING: DNS Integrity Check</td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibCurrentState.0 = INTEGER: minor(3)</td>
<td>IB-TRAP-MIB::ibProbableCause.0 INTEGER: ibDNSIntegrityCheckNameserversFailed(102)</td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibObjectName.0 = STRING: DNSAttack</td>
<td>IB-TRAP-MIB::ibPreviousState.0 = INTEGER: dns-attack-active(115)</td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibPreviousState.0 = INTEGER: dns-attack-inactive(116)</td>
<td>IB-TRAP-MIB::ibTrapDesc.0 = STRING: DNS Integrity Check is unable to connect to any nameservers required to perform the check. There are list of nameservers failure: (['10.35.0.56'])</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>DNS Integrity Check Connection</strong></th>
<th>Sends notifications about whether DNS integrity check connection is functioning or not. For more information, see <strong>ibPreviousState (OID 3.1.1.1.2.9.0) and ibCurrentState (OID 3.1.1.1.2.10.0)</strong>.</th>
<th>016-01-12 05:10:27</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.35.129.15 [UDP: [10.35.129.15]:35201-&gt;[10.120.20.12]]:</td>
<td>DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (213856) 0:35:38.56</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::snmpTrapOID.0 = OID:</td>
<td>IB-TRAP-MIB::ibStateChangeEvent</td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.129.15&quot;</td>
<td>IB-TRAP-MIB::ibCurrentState.0 = INTEGER: dns-integrity-check-severity-informational(99)</td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibCurrentState.0 = INTEGER: dns-integrity-check-severity-indetermined(97)</td>
<td>IB-TRAP-MIB::ibPreviousState.0 = INTEGER: dns-integrity-check-severity-indetermined(97)</td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibObjectName.0 = STRING: DNS Integrity Check</td>
<td>IB-TRAP-MIB::ibTrapDesc.0 = STRING: DNS Integrity Check severity has changed. For DNS zone 'default-com.info', severity has changed from 'NONE' to 'INFORMATIONAL'. Reason: While checking server ib-10-35-133-2.infoblox.com.(ipv4=10.35.133.2) INFORMATIONAL discrepancy found because our servers have record(s): info.com. IN NS ib-10-35-12</td>
</tr>
<tr>
<td>Database</td>
<td>Sends notifications about the database status. For more information, see <em>Processing and Software Failure Traps</em>.</td>
<td>2013-04-05 02:27:01</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (120021) 0:20:00.21</td>
<td>10.35.116.2 [UDP: [10.35.116.2]:45332-&gt;[10.120.20.160]]:</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::snmpTrapOID.0 = OID:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibThresholdCrossingEvent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibNodeName.0 = STRING: “10.35.116.2”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: minor(3)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibObjectName.0 = STRING: db_usage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibCurThresholdValue.0 = INTEGER: 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibThresholdHigh.0 = INTEGER: 85</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibThresholdLow.0 = INTEGER: 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibTrapDesc.0 = STRING: Database capacity used is OK.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disconnected Grid</th>
<th>Sends notifications about whether a Grid has been disconnected from the Master Grid. For more information, see <em>Object State Change Traps</em>.</th>
<th>2011-12-27 23:38:44</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1049) 0:00:10.49</td>
<td>eng-lab-089.inca.infoblox.com [UDP: [10.35.0.89]:53010-&gt;[10.120.20.160]]:</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::snmpTrapOID.0 = OID:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibStateChangeEvent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibNodeName.0 = STRING: “10.35.0.89”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibObjectName.0 = STRING: ID_Grid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibPreviousState.0 = INTEGER: grid-disconnected(5)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibCurrentState.0 = INTEGER: grid-connected(4)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibTrapDesc.0 = STRING: The grid member is connected to the grid master.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Discovery</th>
<th>Sends notifications about the discovery status. For information about the Discovery feature, see <em>Infoblox Network Insight</em>.</th>
<th>2013-10-22 01:35:53</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (122717) 0:20:27.17</td>
<td>eng-lab-302.inca.infoblox.com [UDP: [10.35.1.46]:57126-&gt;[10.120.20.102]]:</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::snmpTrapOID.0 = OID:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibStateChangeEvent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibNodeName.0 = STRING: “10.35.1.46”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibObjectName.0 = STRING: discovery_collector</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibPreviousState.0 = INTEGER: 89</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibCurrentState.0 = INTEGER: 86</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibTrapDesc.0 = STRING: Discovery Collector Service is working.</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Timestamp</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Discovery Conflict</td>
<td>Sends notifications about conflicts between the DHCP address and the existing IP address. For more information, see <em>Processing and Software Failure Traps</em>.</td>
<td>2014-06-20 00:48:06</td>
</tr>
<tr>
<td>Discovery Unmanaged</td>
<td>Sends notifications related to the discovery of unmanaged devices and networks. You can configure the maximum number of unmanaged objects the appliance discovers and how often it notifies about these events. For more information about how to configure these parameters, see <em>Defining Seed Routers for Probe Members</em>.</td>
<td>2015-02-09 22:53:57</td>
</tr>
<tr>
<td>Disk</td>
<td>Sends notifications about the status of the primary disk. For more information, see <em>Threshold Crossing Traps</em>.</td>
<td>2012-11-22 03:34:32</td>
</tr>
</tbody>
</table>
| **DuplicateIP** | Sends notifications when there are duplicate IP addresses. For more information, see `ibProbableCause Values` (OID 3.1.1.1.2.4.0). | 2016-04-18 22:47:38  
10.35.139.15 [UDP: [10.35.139.15]:35531->[10.120.21.204]]:  
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (7239201)  
20:06:32.01  
SNMPv2-MIB::snmpTrapOID.0 = OID:  
IB-TRAP-MIB::ibProcessingFailureTrap  
IB-TRAP-MIB::ibNodeName.0 = STRING: "10.35.139.15"  
IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: major(4)  
IB-TRAP-MIB::ibSubsystemName.0 = STRING: Equipment  
IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibDuplicateIPAddressFailure(52)  
IB-TRAP-MIB::ibTrapDesc.0 = STRING: A Duplicate IP Address has been detected. |
| **ENAT** | Sends notifications about the Ethernet port status. For more information, see `ibPreviousState (OID 3.1.1.1.2.9.0)` and `ibCurrentState (OID 3.1.1.1.2.10.0)`. | 2012-08-27 03:05:25  
10.36.3.132 [UDP: [10.36.3.132]:47962->[10.120.20.232]]:  
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (16624)  
0:02:46.24  
SNMPv2-MIB::snmpTrapOID.0 = OID:  
IB-TRAP-MIB::ibStateChangeEvent  
IB-TRAP-MIB::ibNodeName.0 = STRING: "10.35.3.132"  
IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: major(4)  
IB-TRAP-MIB::ibObjectName.0 = STRING: LAN  
IB-TRAP-MIB::ibPreviousState.0 = INTEGER: enet-link-up(6)  
IB-TRAP-MIB::ibCurrentState.0 = INTEGER: enet-link-down(7)  
IB-TRAP-MIB::ibTrapDesc.0 = STRING: LAN1 port link is down. Please check the connection. |
| **File Distribution Usage** | Sends notifications about the HTTP file distribution process. For more information, see `Processing and Software Failure Traps`. | 2016-01-08 01:48:57  
10.40.240.113 [UDP: [10.40.240.113]:41443->[10.120.20.21]]:  
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (183757)  
0:30:37.57  
SNMPv2-MIB::snmpTrapOID.0 = OID:  
IB-TRAP-MIB::ibProcessingFailureTrap  
IB-TRAP-MIB::ibNodeName.0 = STRING: "10.40.240.113"  
IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: critical(5)  
IB-TRAP-MIB::ibSubsystemName.0 = STRING: fd_usage  
IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibFDSoftwareFailure(42)  
IB-TRAP-MIB::ibTrapDesc.0 = STRING: File Distribution services storage usage is OK. |
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Event Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>Sends notifications about the status of FTP service. For more information, see <a href="#">Processing and Software Failure Traps</a>.</td>
<td>2016-01-07 23:27:22 10.40.240.113 [UDP: [10.40.240.113]:36063-&gt;[10.120.20.21]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (380473) 1:03:24.73 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibProcessingFailureTrap IB-TRAP-MIB::ibNodeName.0 = STRING: “10.40.240.113” IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: critical(5) IB-TRAP-MIB::ibSubsystemName.0 = STRING: ftp IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibFTPDSoftwareFailure(44) IB-TRAP-MIB::ibTrapDesc.0 = STRING: An FTPD daemon failure has occurred.</td>
</tr>
<tr>
<td>Fan</td>
<td>Sends notifications about the status of the system fan. For more information, see <a href="#">Equipment Failure Traps</a>.</td>
<td>2012-02-23 23:34:50 10.32.1.222 [UDP: [10.32.1.222]:42742-&gt;[10.35.109.24]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (89508) 0:14:55.08 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibEquipmentFailureTrap IB-TRAP-MIB::ibNodeName.0 = STRING: “10.32.1.222” IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: minor(3) IB-TRAP-MIB::ibObjectName.0 = STRING: fan IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibFan1Failure(37) IB-TRAP-MIB::ibTrapDesc.0 = STRING: Fan 1 failure has occurred.</td>
</tr>
<tr>
<td>HA</td>
<td>Sends notifications about the status of the HA port link. For more information, see <a href="#">ibPreviousState (OID 3.1.1.2.9.0) and ibCurrentState (OID 3.1.1.2.10.0)</a>.</td>
<td>2014-05-23 00:49:32 eng-lab-589.inca.infoblox.com [UDP: [10.35.2.77]:46426-&gt;[10.36.0.200]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (3912) 0:00:39.12 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibStateChangeEvent IB-TRAP-MIB::ibNodeName.0 = STRING: “10.35.20.70” IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2) IB-TRAP-MIB::ibObjectName.0 = STRING: HA_Replication IB-TRAP-MIB::ibPreviousState.0 = INTEGER: ha-replication-offline(14) IB-TRAP-MIB::ibCurrentState.0 = INTEGER: ha-replication-online(13) IB-TRAP-MIB::ibTrapDesc.0 = STRING: HA replication is online.</td>
</tr>
<tr>
<td>Service</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
</tbody>
</table>
| HSM | Sends notifications about the status of the HSM operation. For more information, see `ibPreviousState (OID 3.1.1.1.2.9.0)` and `ibCurrentState (OID 3.1.1.1.2.10.0)`. | 2016-01-12 | 20:52:12 | 10.39.13.77 [UDP: [10.39.13.77]:44962->[10.120.20.21]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (131909) 0:21:59.09
SNMPv2-MIB::snmpTrapOID.0 = OID:
IB-TRAP-MIB::ibStateChangeEvent
IB-TRAP-MIB::ibNodeName.0 = STRING: "10.39.13.77"
IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2)
IB-TRAP-MIB::ibObjectName.0 = STRING: DNS
IB-TRAP-MIB::ibPreviousState.0 = INTEGER: dns-service-working(32)
IB-TRAP-MIB::ibCurrentState.0 = INTEGER: 55
IB-TRAP-MIB::ibTrapDesc.0 = STRING: DNS Service restarted not using HSM |
| HTTP | Sends notifications about the status of the HTTP service. For more information, see `ibPreviousState (OID 3.1.1.1.2.9.0)` and `ibCurrentState (OID 3.1.1.1.2.10.0)`. | 2016-01-07 | 23:16:40 | 10.40.240.113 [UDP: [10.40.240.113]:36063->[10.120.20.21]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (316247) 0:52:42.47
SNMPv2-MIB::snmpTrapOID.0 = OID:
IB-TRAP-MIB::ibStateChangeEvent
IB-TRAP-MIB::ibNodeName.0 = STRING: "10.40.240.113"
IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2)
IB-TRAP-MIB::ibObjectName.0 = STRING: http_file_dist
IB-TRAP-MIB::ibPreviousState.0 = INTEGER: http-file-dist-service-inactive(40)
IB-TRAP-MIB::ibCurrentState.0 = INTEGER: http-file-dist-service-working(38)
IB-TRAP-MIB::ibTrapDesc.0 = STRING: HTTP File Dist Service is working |
| IFMAP | Sends notifications about the status of the IF-MAP service. For more information, see `ibProbableCause Values (OID 3.1.1.1.2.4.0)`. | 2016-04-20 | 23:40:00 | 10.34.41.60 [UDP: [10.34.41.60]:33231->[10.120.21.204]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (45256) 0:07:32.56
SNMPv2-MIB::snmpTrapOID.0 = OID:
IB-TRAP-MIB::ibProcessingFailureTrap
IB-TRAP-MIB::ibNodeName.0 = STRING: "10.34.41.60"
IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: critical(5)
IB-TRAP-MIB::ibSubsystemName.0 = STRING: ifmapd
IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ifmapdSoftwareFailure(50)
IB-TRAP-MIB::ibTrapDesc.0 = STRING: An IF-MAP server failure has occurred. |
<p>| IPMI Device | Sends notifications about the status of the IPMI device. For more information, see <code>ibProbableCause Values</code> (OID 3.1.1.1.2.4.0). | 2015-03-24 04:10:21 eng-lab-598.inca.infoblox.com [UDP: [10.35.2.86]:56092-&gt;[10.120.20.21]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (103490) 0:17:14.90 SNMPv2-MIB::snmpTrapOID.0 = OID: ib-TRAP-MIB::ibOperationTrap ib-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.2.86&quot; ib-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2) ib-TRAP-MIB::ibSubsystemName.0 = STRING: IPMI Status Check IB-TRAP-MIB::ibProbableCause.0 = INTEGER: 2105 ib-TRAP-MIB::ibTrapDesc.0 = STRING: IPMI is used by some hardware monitors to test hardware health. The IPMI Device is now available; subsequent hardware monitor failures are likely to be genuine. |
| IPAM Utilization | Sends notifications about the percentage of IPv4 addresses that are used in a network. For a network container that contains subnets, this indicates the percentage of the total address space defined within the container regardless of whether any of the IP addresses are used in the subnetwork. For more information, see <code>Threshold Crossing Traps</code>. | 2014-07-06 19:33:01 eng-lab-514.inca.infoblox.com [UDP: [10.35.2.2]:33413-&gt;[10.120.20.21]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1038846) 2:53:08.46 SNMPv2-MIB::snmpTrapOID.0 = OID: ib-TRAP-MIB::ibThresholdCrossingEvent ib-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.2.2&quot; ib-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2) ib-TRAP-MIB::ibObjectName.0 = STRING: Threshold ib-TRAP-MIB::ibCurThresholdValue.0 = INTEGER: 0 ib-TRAP-MIB::ibThresholdHigh.0 = INTEGER: 5 ib-TRAP-MIB::ibThresholdLow.0 = INTEGER: 3 ib-TRAP-MIB::ibTrapDesc.0 = STRING: Network IPAM Utilization capacity usage is OK. Network: 20.0.0.0/29/netview |
| Load Balancer Device | Sends notifications about whether the LB device is in sync or not. For more information, see <code>ibPreviousState (OID 3.1.1.1.2.9.0)</code> and <code>ibCurrentState (OID 3.1.1.1.2.10.0)</code>. | 2013-07-08 02:36:39 10.35.113.2 [UDP: [10.35.113.2]:45568-&gt;[10.120.20.21]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (996274) 2:46:02.74 SNMPv2-MIB::snmpTrapOID.0 = OID: ib-TRAP-MIB::ibStateChangeEvent ib-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.113.2&quot; ib-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2) ib-TRAP-MIB::ibObjectName.0 = STRING: device ib-TRAP-MIB::ibPreviousState.0 = INTEGER: lb-device-down(74) ib-TRAP-MIB::ibCurrentState.0 = INTEGER: lb-device-up(73) ib-TRAP-MIB::ibTrapDesc.0 = STRING: Load Balancer device 10.36.128.1 sync is OK. |</p>
<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Date Time</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCD</td>
<td>Sends notifications about the status of the LCD process. For more information, see Processing and Software Failure Traps.</td>
<td>2011-12-01 06:31:28</td>
<td>ib-10-35-3-125.infoblox.com [UDP: [10.35.3.125]:56609-&gt;[10.35.3.125]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (187334) 0:31:13.34 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibProcessingFailureTrap IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.3.125&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: major(4) IB-TRAP-MIB::ibSubsystemName.0 = STRING: lcd IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibLCDSoftwareFailure(18) IB-TRAP-MIB::ibTrapDesc.0 = STRING: An LCD failure has occurred.</td>
</tr>
<tr>
<td>LDAP Servers</td>
<td>Sends notifications about whether LDAP servers are available or not. For more information, see ibPreviousState (OID 3.1.1.1.2.9.0) and ibCurrentState (OID 3.1.1.1.2.10.0).</td>
<td>2012-12-17 03:33:58</td>
<td>10.35.106.6 [UDP: [10.35.106.6]:35751-&gt;[10.120.20.249]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (4043) 0:00:40.43 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibStateChangeEvent IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.106.6&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2) IB-TRAP-MIB::ibObjectName.0 = STRING: ldap_servers IB-TRAP-MIB::ibPreviousState.0 = INTEGER: ldap-service-inactive(79) IB-TRAP-MIB::ibCurrentState.0 = INTEGER: ldap-servers-ok(76) IB-TRAP-MIB::ibTrapDesc.0 = STRING: All LDAP servers are available.</td>
</tr>
<tr>
<td>License</td>
<td>Sends notifications when the license has been revoked. For more information, see Revoked License Trap.</td>
<td>2014-05-23 00:49:32</td>
<td>eng-lab-589.inca.infoblox.com [UDP: [10.35.2.77]:46426-&gt;[10.36.0.200]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (3912) 0:00:39.12 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibTrapOneModule.6.0 IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.34.156.165&quot; IB-TRAP-MIB::ibSubsystemName.0 = STRING: vnios IB-TRAP-MIB::ibTrapDesc.0 = STRING: Grid license of member IP 10.34.196.165 with hardware ID 564d5c2115391ab3f6efee9a9d974aa is revoked. 0 Cold Start</td>
</tr>
<tr>
<td>Login</td>
<td>Sends notifications when the login details are incorrect. For more information, see Processing and Software Failure Traps.</td>
<td>2013-04-30 02:56:49</td>
<td>10.34.132.2 [UDP: [10.34.132.2]:35433-&gt;[10.120.20.160]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (27604) 0:04:36.04 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibProcessingFailureTrap IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.34.152.2&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: minor(3) IB-TRAP-MIB::ibSubsystemName.0 = STRING: Login IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibGUILoginFailure(58) IB-TRAP-MIB::ibTrapDesc.0 = STRING: A GUI login failure has occurred.</td>
</tr>
</tbody>
</table>
MGM  Sends notifications about the status of the multi-Grid configuration. For more information, see `ibPreviousState (OID 3.1.1.1.2.9.0)` and `ibCurrentState (OID 3.1.1.1.2.10.0)`.

2013-04-03 23:48:34
eng-lab-482.inca.infoblox.com [UDP: [10.35.1.226]:37893->[10.120.20.160]]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (24697)
0:04:06.97
SNMPv2-MIB::snmpTrapOID.0 = OID:
IB-TRAP-MIB::ibTrapOneModule.4
IB-TRAP-MIB::ibNodeName.0 = STRING: "10.35.116.2"
IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: major(4)
IB-TRAP-MIB::ibObjectName.0 = STRING: Grid of Grids
IB-TRAP-MIB::ibPreviousState.0 = INTEGER: 23
IB-TRAP-MIB::ibCurrentState.0 = INTEGER: 24
IB-TRAP-MIB::ibTrapDesc.0 = STRING: Grid connection offline.

MSServer  Sends notifications about the status of Microsoft Servers for Microsoft management. For more information, see `ibPreviousState (OID 3.1.1.1.2.9.0)` and `ibCurrentState (OID 3.1.1.1.2.10.0)`.

2013-07-10 03:29:42
10.35.113.2 [UDP: [10.35.113.2]:51679->[10.120.20.21]]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1066392)
2:57:43.92
SNMPv2-MIB::snmpTrapOID.0 = OID:
IB-TRAP-MIB::ibStateChangeEvent
IB-TRAP-MIB::ibNodeName.0 = STRING: "10.35.113.2"
IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2)
IB-TRAP-MIB::ibObjectName.0 = STRING: ms_service
IB-TRAP-MIB::ibPreviousState.0 = INTEGER: ms-service-down(20)
IB-TRAP-MIB::ibCurrentState.0 = INTEGER: ms-service-up(19)
IB-TRAP-MIB::ibTrapDesc.0 = STRING: Service connection to Microsoft DNS server 10.102.31.67 is OK.

Memory  Sends notifications about the status of the system memory. For more information, see `Threshold Crossing Traps`.

2012-04-17 03:09:46
10.35.119.4 [UDP: [10.35.119.4]:37664->[10.120.20.160]]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (359835)
0:59:58.35
SNMPv2-MIB::snmpTrapOID.0 = OID:
IB-TRAP-MIB::ibTrapOneModule.3
IB-TRAP-MIB::ibNodeName.0 = STRING: "10.35.119.4"
IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: minor(3)
IB-TRAP-MIB::ibObjectName.0 = STRING: memory
IB-TRAP-MIB::ibCurThresholdValue.0 = INTEGER: 46
IB-TRAP-MIB::ibThresholdHigh.0 = INTEGER: 50
IB-TRAP-MIB::ibThresholdLow.0 = INTEGER: 30
IB-TRAP-MIB::ibTrapDesc.0 = STRING: System memory usage is OK.
<table>
<thead>
<tr>
<th><strong>NTP</strong></th>
<th>Sends notifications about the status of the NTP service. For more information, see <code>ibPreviousState (OID 3.1.1.1.2.9.0)</code> and <code>ibCurrentState (OID 3.1.1.1.2.10.0)</code></th>
<th>2013-04-02 23:58:19</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.35.116.6 [UDP: [10.35.116.6]:37505-&gt;[10.120.20.160]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (17804) 0:02:58.04 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibStateChangeEvent IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.1.187&quot; IB-TRAP-MIB::ibObjectName.0 = STRING: ntp_sync IB-TRAP-MIB::ibPreviousState.0 = INTEGER: ntp-sync-down(16) IB-TRAP-MIB::ibCurrentState.0 = INTEGER: ntp-sync-up(15) IB-TRAP-MIB::ibTrapDesc.0 = STRING: The NTP service resumed synchronization.</td>
<td></td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>Sends notifications about the status of the LAN port. For more information, see <em>Threshold Crossing Traps</em>.</td>
<td>2013-01-06 23:52:01</td>
</tr>
<tr>
<td></td>
<td>10.35.3.62 [UDP: [10.35.3.62]:49255-&gt;[10.120.20.160]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (80879) 0:13:28.79 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibTrapOneModule.3 IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.3.62&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: minor(3) IB-TRAP-MIB::ibObjectName.0 = STRING: MGM IB-TRAP-MIB::ibCurThresholdValue.0 = INTEGER: 8 IB-TRAP-MIB::ibThresholdHigh.0 = INTEGER: 5 IB-TRAP-MIB::ibThresholdLow.0 = INTEGER: 3 IB-TRAP-MIB::ibTrapDesc.0 = STRING: Network capacity used is over the threshold value.</td>
<td></td>
</tr>
<tr>
<td><strong>OCSP Responders</strong></td>
<td>Sends notifications about the status of OCSP responders. For more information, see <code>ibPreviousState (OID 3.1.1.1.2.9.0)</code> and <code>ibCurrentState (OID 3.1.1.1.2.10.0)</code>.</td>
<td>2016-01-14 03:21:14</td>
</tr>
<tr>
<td></td>
<td>10.34.9.91 [UDP: [10.34.9.91]:34663-&gt;[10.120.21.204]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (4599) 0:00:45.99 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibStateChangeEvent IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.34.9.91&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2) IB-TRAP-MIB::ibObjectName.0 = STRING: ocsp_responders IB-TRAP-MIB::ibPreviousState.0 = INTEGER: ocsp-responders-ok(65) IB-TRAP-MIB::ibCurrentState.0 = INTEGER: ocsp-service-inactive(68) IB-TRAP-MIB::ibTrapDesc.0 = STRING: OCSP service inactive.</td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>Sends notifications about the ospfd process. For more information, see <em>Proces sing and Software Failure Traps</em>.</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2012-11-22 04:49:56 eng-lab-883.inca.infoblox.com [UDP: [10.35.3.115]:38185-&gt;[10.120.20.160]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (50414) 0:08:24.14 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibTrapOneModule.2 IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.3.115&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: critical(5) IB-TRAP-MIB::ibSubsystemName.0 = STRING: ospf IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibOSPFSoftwareFailure(35) IB-TRAP-MIB::ibTrapDesc.0 = STRING: An OSPF routing daemon failure has occurred.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OSPF6</th>
<th>Sends notifications about the ospf process for IPv6. For more information, see <em>ibProbableCause Values</em> (OID 3.1.1.1.2.4.0).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2016-01-13 02:03:07 eng-lab-396.inca.infoblox.com [UDP: [10.35.1.140]:45733-&gt;[10.120.20.21]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (3970) 0:00:39.70 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibProcessingFailureTrap IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.1.140&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: minor(3) IB-TRAP-MIB::ibSubsystemName.0 = STRING: ospf6 IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibClear(0) IB-TRAP-MIB::ibTrapDesc.0 = STRING: SNMP Trap is cleared. OSPF6 SW</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PowerSupply</th>
<th>Sends notifications about the status of the power supply. For more information, see <em>Equipment Failure Traps</em>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2012-01-20 22:45:01 nextgen.com [UDP: [10.32.111.110]:45323-&gt;[10.32.111.110]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (21044) 0:03:30.44 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibEquipmentFailureTrap IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.32.111.110&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2) IB-TRAP-MIB::ibObjectName.0 = STRING: power_supply IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibSystemRestart(61) IB-TRAP-MIB::ibTrapDesc.0 = STRING: Power supply 2 is OK.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RAID</th>
<th>Sends notifications about the RAID array status. For more information, see <em>Equipment Failure Traps</em>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2016-01-15 14:30:20 eng-lab-418.inca.infoblox.com [UDP: [10.35.1.162]:57616-&gt;[10.120.21.204]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8737) 0:01:27.37 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibEquipmentFailureTrap IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.1.162&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: major(4) IB-TRAP-MIB::ibObjectName.0 = STRING: raid IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibRAIDisDegraded(3002) IB-TRAP-MIB::ibTrapDesc.0 = STRING: The system's RAID array is in a degraded state.</td>
</tr>
<tr>
<td>Recursive Clients</td>
<td>Sends notifications about whether the DNS recursive server is under flood attacks. For more information, see <em>Threshold Crossing Traps</em>.</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>2015-01-13 02:05:55 eng-lab-078.inca.infoblox.com [UDP: [10.35.0.78]:55233-&gt;[10.120.20.21]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (168817) 0:28:08.17 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibThresholdCrossingEvent IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.35.0.78&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: minor(3) IB-TRAP-MIB::ibObjectName.0 = STRING: RecursiveClients IB-TRAP-MIB::ibCurThresholdValue.0 = INTEGER: 1 IB-TRAP-MIB::ibThresholdHigh.0 = INTEGER: 800 IB-TRAP-MIB::ibThresholdLow.0 = INTEGER: 300 IB-TRAP-MIB::ibTrapDesc.0 = STRING: Number of simultaneous DNS recursive lookups is OK.</td>
</tr>
<tr>
<td>RIR SWIP</td>
<td>Sends notifications about the status of the RIR SWIP registration. For more information, see <em>ibProbableCause Values</em> (OID 3.1.1.1.2.4.0).</td>
</tr>
<tr>
<td></td>
<td>2016-01-11 02:05:17 10.34.11.100 [UDP: [10.34.11.100]:52957-&gt;[10.120.21.204]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (43623) 0:07:16.23 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibProcessingFailureTrap IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.34.11.100&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: major(4) IB-TRAP-MIB::ibSubsystemName.0 = STRING: RIR SWIP IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibRIRSWIPRegistrationFailure(89) IB-TRAP-MIB::ibTrapDesc.0 = STRING: An RIR SWIP registration failure has occurred.CRE Are RIR registration request for network &quot;187.0.0.0/24&quot; failed.</td>
</tr>
<tr>
<td>Reporting</td>
<td>Sends notifications about the status of the reporting database. For more information, see <em>Threshold Crossing Traps</em>.</td>
</tr>
<tr>
<td></td>
<td>2012-01-06 08:59:55 10.35.101.27 [UDP: [10.35.101.27]:59714-&gt;[10.35.117.24]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (289200) 0:48:12.00 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibThresholdCrossingEvent IB-TRAP-MIB::ibNodeName.0 = STRING: &quot;10.34.46.6&quot; IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: minor(3) IB-TRAP-MIB::ibObjectName.0 = STRING: reporting_volume IB-TRAP-MIB::ibCurThresholdValue.0 = INTEGER: 85 IB-TRAP-MIB::ibThresholdHigh.0 = INTEGER: 80 IB-TRAP-MIB::ibThresholdLow.0 = INTEGER: 71 IB-TRAP-MIB::ibTrapDesc.0 = STRING: Reporting volume usage reached the threshold value.</td>
</tr>
<tr>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RPZ Hit Rate</td>
<td>Send Notifications about the percentage of RPZ Hit Rate. For more information, see Threshold Crossing Traps.</td>
</tr>
<tr>
<td>RootFS</td>
<td>Sends notifications about the status of the root file system. For more information, see Threshold Crossing Traps.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Sends notifications about the status of the SNMP server. For more information, see Processing and Software Failure Traps.</td>
</tr>
<tr>
<td>SSH</td>
<td>Sends notifications about the status of the <code>sshd</code> process. For more information, see <em>Processing and Software Failure Traps</em>.</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>2011-09-21 21:33:17 10.34.42.6 [UDP: [10.34.42.6]:49776-&gt;[10.34.42.2]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (6508) 0:01:05.08 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibProcessingFailureTrap IB-TRAP-MIB::ibNodeName.0 = STRING: “10.34.42.6” IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: minor(3) IB-TRAP-MIB::ibSubsystemName.0 = STRING: ssh IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibClear(0) IB-TRAP-MIB::ibTrapDesc.0 = STRING: SNMP Trap is cleared. SSHD SW</td>
</tr>
<tr>
<td>SerialConsole</td>
<td>Sends notifications when the serial console login has failed or the admin failed to login to the serial console. For more information, see <em>Processing and Software Failure Traps</em>.</td>
</tr>
<tr>
<td></td>
<td>2014-12-15 02:47:59 UDP/IPv6: 2620:10a:6000:2400::8104]:55038 [UDP/IPv6: [2620:10a:6000:2400::8104]:55038]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (501585) 1:23:35.85 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibProcessingFailureTrap IB-TRAP-MIB::ibNodeName.0 = STRING: “2620:10a:6000:2400::8104” IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: minor(3) IB-TRAP-MIB::ibSubsystemName.0 = STRING: Login IB-TRAP-MIB::ibProbableCause.0 = INTEGER: ibSerialConsoleLoginFailure(59) IB-TRAP-MIB::ibTrapDesc.0 = STRING: A Serial Console login failure has occurred.</td>
</tr>
<tr>
<td>Swap Usage</td>
<td>Sends notifications about whether the swap usage has exceeded the trigger or reset value. For more information, see <em>Defining Thresholds for Traps</em>.</td>
</tr>
<tr>
<td></td>
<td>2013-11-25 05:35:56 10.35.129.1 [UDP: [10.35.129.1]:49489-&gt;[10.120.20.21]]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (24009) 0:04:00.09 SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibThresholdCrossingEvent IB-TRAP-MIB::ibNodeName.0 = STRING: “10.35.129.1” IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: major(4) IB-TRAP-MIB::ibObjectName.0 = STRING: swap_usage IB-TRAP-MIB::ibCurThresholdValue.0 = INTEGER: 100 IB-TRAP-MIB::ibThresholdHigh.0 = INTEGER: 5 IB-TRAP-MIB::ibThresholdLow.0 = INTEGER: 2 IB-TRAP-MIB::ibTrapDesc.0 = STRING: System swap space usage exceeds the critical threshold value.</td>
</tr>
<tr>
<td>Service</td>
<td>Sends notifications when the syslog process stops. For more information, see Processing and Software Failure Traps.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>System</td>
<td>Sends notifications about the status of the NIOS system. For more information, see Process Started and Stopped Traps.</td>
</tr>
<tr>
<td>TAXII</td>
<td>Sends notifications when you start and stop the TAXII service. For more information, see Object State Change Traps.</td>
</tr>
<tr>
<td>TFTP</td>
<td>Sends notifications about the status of the TFTP service. For more information, see Processing and Software Failure Traps.</td>
</tr>
<tr>
<td>Threat Analytics</td>
<td>Sends notifications about the status of the Threat Analytics service. For more information, see [ibProbableCause Values](# OID 3.1.1.1.2.4.0).</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>10.35.3.154 [UDP: [10.35.3.154]:59876-&gt;[10.120.20.12]]; DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (16184) 0:02:41.84</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibStateChangeEvent IB-TRAP-MIB::ibNodeName.0 = STRING: “10.35.3.154”</td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2) IB-TRAP-MIB::ibObjectName.0 = STRING: Threat Analytics IB-TRAP-MIB::ibPreviousState.0 = INTEGER: 127</td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibCurrentState.0 = INTEGER: 126 IB-TRAP-MIB::ibTrapDesc.0 = STRING: Threat Analytics Service is working.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat Analytics</th>
<th>Sends notifications about the DNS tunneling detection. For more information, see [ibProbableCause Values](# OID 3.1.1.1.2.4.0).</th>
<th>2016-01-08 00:22:07</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.35.3.154 [UDP: [10.35.3.154]:59876-&gt;[10.120.20.12]]; DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (31567) 0:05:15.67</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibOperationTrap IB-TRAP-MIB::ibNodeName.0 = STRING: “10.35.3.154”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: major(4) IB-TRAP-MIB::ibSubsystemName.0 = STRING: Software IB-TRAP-MIB::ibProbableCause.0 = INTEGER: 4013</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibTrapDesc.0 = STRING: DNS Tunneling detected: The record '*.any.knuqjysfyc2t.com' is successfully added into BlockList RPZ zone with comment '[2016-08-01 08:22:06 UTC] [member: infoblox.localdomain] DNS Tunneling' and policy 'No Data'.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat Protection</th>
<th>Sends notifications about whether the threat protection service for Infoblox DNS Protection is functioning properly. For more information, see [ibPreviousState](# OID 3.1.1.1.2.9.0) and [ibCurrentState](# OID 3.1.1.1.2.10.0)</th>
<th>2016-04-18 22:48:08</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.35.139.15 [UDP: [10.35.139.15]:54407-&gt;[10.120.21.204]]; DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (3926) 0:00:39.26</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::snmpTrapOID.0 = OID: IB-TRAP-MIB::ibStateChangeEvent IB-TRAP-MIB::ibNodeName.0 = STRING: “10.35.139.15”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibTrapSeverity.0 = INTEGER: info(2) IB-TRAP-MIB::ibObjectName.0 = STRING: threat_protection IB-TRAP-MIB::ibPreviousState.0 = INTEGER: threat-protection-service-inactive(93)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IB-TRAP-MIB::ibCurrentState.0 = INTEGER: threat-protection-service-inactive(93) IB-TRAP-MIB::ibTrapDesc.0 = STRING: Threat Protection Service is inactive.</td>
<td></td>
</tr>
</tbody>
</table>

### Testing the SNMP Configuration

After you configure SNMP on the appliance, you can do the following to test your SNMP configuration:

- From the Grid tab, select the Grid Manager tab -> Members tab -> Grid_member check box, and then select Test SNMP from the Toolbar.
The appliance sends a “test trap” string to the trap receiver and displays a confirmation message at the top of the screen if your SNMP configuration is properly set up. If your SNMP configuration is not complete or if it is invalid, the appliance displays an error message. You can check your configuration and try again.

The following is a sample test trap that the trap receiver can get:

```
2011-04-04 17:37:14 10.32.2.80 [UDP: 10.32.2.80]:49244->[10.32.2.80]]:
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::snmpTrapOID
SNMPv2-MIB::sysName.0 = STRING: 'Test trap'
```

SNMP MIB Hierarchy

In addition to implementing its own enterprise MIBs, Infoblox supports the standard MIBs defined in RFC-1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II.

The Infoblox MIBs are part of a universal hierarchical structure, usually referred to as the MIB tree. The MIB tree has an unlabeled root with three subtrees. Figure 39.2 illustrates the branch of the MIB tree that leads to the Infoblox enterprise MIBs. Each object in the MIB tree has a label that consists of a textual description and an OID (object identifier). An OID is a unique dotted-decimal number that identifies the location of the object in the MIB tree. Note that all OIDs begin with a dot (.) to indicate the root of the MIB tree.

As shown in Figure 39.2, Infoblox is a branch of the Enterprise subtree. IANA (Internet Assigned Numbers Authority) administers the Enterprise subtree, which is designated specifically for vendors who define their own MIBs. The IANA-assigned enterprise number of Infoblox is 7779; therefore, the OIDs of all Infoblox MIB objects begin with the prefix .1.3.6.1.4.1.7779. In addition, IB-DNSSERV and IB-DHCPserv are branches of the Enterprise subtree as well.

The Infoblox SNMP subtree branches down through two levels, ibProduct and ibOne, to the Infoblox MIBs: ibTrap, ibPlatformOne, ibDNSOne, and ibDHCPOne. The ibTrap MIB defines the traps that NIOS appliances send, and the ibPlatformOne, ibDNSOne, and ibDHCPOne MIBs provide information about the appliance. For detailed information about these MIBs, see Infoblox MIBs.
The Infoblox MIB objects were implemented according to the guidelines in RFCs 1155 and 2578. They specify two types of macros for defining MIB objects: OBJECT-TYPE and NOTIFICATION-TYPE. These macros contain clauses that describe the characteristics of an object, such as its syntax and its status. OBJECT-TYPE macros describe MIB objects, and NOTIFICATION-TYPE macros describe objects used in SNMP traps. Each object in the ibPlatformOne, ibDNSOne, and ibDHCPOne MIBs contains the following clauses from the OBJECT-TYPE macro:

- **OBJECT-TYPE**: Provides the administratively-assigned name of the object.
- **SYNTAX**: Identifies the data structure of the object, such as integers, counters, and octet strings.
- **MAX-ACCESS**: Identifies the type of access that a management station has to the object. All Infoblox MIB objects provide read-only access.
- **STATUS**: Identifies the status of the object. Values are current, obsolete, and deprecated.
- **DESCRIPTION**: Provides a textual description of the object.
- **INDEX or AUGMENTS**: An object that represents a conceptual row must have either an INDEX or AUGMENTS clause that defines a key for selecting a row in a table.
- **OID**: The dotted decimal object identifier that defines the location of the object in the universal MIB tree.

The ibTrap MIB defines the SNMP traps that a NIOS appliance can send. Each object in the ibTrap MIB contains the following clauses from the NOTIFICATION-TYPE macro:

- **NOTIFICATION-TYPE**: Provides the administratively-assigned name of the object.
- OBJECTS: Provides an ordered list of MIB objects that are in the trap.
- STATUS: Identifies the status of the object. Values are current, obsolete, and deprecated.
- DESCRIPTION: Provides the notification information.

System Object IDs

Infoblox uses the SNMP system object identifier `sysObjectID` to identify Infoblox appliances. The following is a definition of `sysObjectID` from the SNMPv2 MIB, `Management Information Base (MIB)` for the `Simple Network Management Protocol (SNMP)`:

<table>
<thead>
<tr>
<th>OBJECT-TYPE</th>
<th>sysObjectID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYNTAX</td>
<td>Object Identifier</td>
</tr>
<tr>
<td>MAX-ACCESS</td>
<td>read-only</td>
</tr>
<tr>
<td>STATUS</td>
<td>current</td>
</tr>
</tbody>
</table>
| DESCRIPTION  | "The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones,Inc.' was assigned the subtree 1.3.6.1.4.1.424242, it could assign the identifier 1.3.6.1.4.1.424242.1.1 to its 'Fred Router'."

Table 39.3 lists the enterprise IDs and their corresponding Infoblox hardware platforms that an SNMP query can return when you request the `sysObjectID` value. Note that the IDs shown in the table do not include 1.3.6.1.4.1.7779.1. (the `infobloxProducts` prefix).

Table 39.3 sysObjectID for Infoblox Hardware

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>ibDefault</td>
<td>Default environments, such as chroot</td>
</tr>
<tr>
<td>1001</td>
<td>ibRsp2</td>
<td>vNIOS appliances on Riverbed Services Platforms</td>
</tr>
<tr>
<td>1002</td>
<td>ibCisco</td>
<td>Cisco servers</td>
</tr>
<tr>
<td>1003</td>
<td>ibvm</td>
<td>vNIOS appliances on VMware ESX or ESXi servers</td>
</tr>
<tr>
<td>1004</td>
<td>ibvnios</td>
<td>Virtual NIOS</td>
</tr>
<tr>
<td>1401</td>
<td>ib810</td>
<td>Trinzic 810 appliances</td>
</tr>
<tr>
<td>1402</td>
<td>ib820</td>
<td>Trinzic 820 appliances</td>
</tr>
<tr>
<td>1403</td>
<td>ib1410</td>
<td>Trinzic 1410 appliances</td>
</tr>
<tr>
<td>1404</td>
<td>ib1420</td>
<td>Trinzic 1420 appliances</td>
</tr>
<tr>
<td>1405</td>
<td>ib1400</td>
<td>Trinzic Reporting 1400 appliances</td>
</tr>
<tr>
<td>1406</td>
<td>ib800</td>
<td>Trinzic Reporting 800 appliances</td>
</tr>
<tr>
<td>1407</td>
<td>pt1400</td>
<td>Advanced 1400 appliances</td>
</tr>
<tr>
<td>1411</td>
<td>ib2200</td>
<td>Trinzic Reporting 2200 appliances</td>
</tr>
<tr>
<td>1412</td>
<td>ib2210</td>
<td>Trinzic 2210 appliances</td>
</tr>
<tr>
<td>1413</td>
<td>ib2220</td>
<td>Trinzic 2220 appliances</td>
</tr>
<tr>
<td>1414</td>
<td>pt2200</td>
<td>Advanced 2200 appliances</td>
</tr>
<tr>
<td>1421</td>
<td>ib4010</td>
<td>Infoblox-4010 appliances</td>
</tr>
<tr>
<td>1422</td>
<td>ib4030</td>
<td>Infoblox-4030 appliances</td>
</tr>
<tr>
<td>1423</td>
<td>ib4000</td>
<td>Infoblox-4000 appliances</td>
</tr>
<tr>
<td>1424</td>
<td>pt4000</td>
<td>Advanced 4000 appliances</td>
</tr>
</tbody>
</table>
Infoblox MIBs

You can configure a NIOS appliance as an SNMP-managed device so that an SNMP management station can send queries to the appliance and retrieve information from its MIBs. Perform the following tasks to access the Infoblox MIBs:

1. Configure a NIOS appliance to accept queries, as described in [Configuring SNMPv3 Users](#).
2. Load the MIB files onto the management system. To obtain the latest Infoblox MIB files:
   a. From the Data Management tab, select the Grid tab -> Grid Manager tab, and then select Download -> SNMP MIBs from the Toolbar.
   b. In the Save As dialog box, navigate to a directory to which you want to save the MIBs.
   c. Click Save.
3. Use a MIB browser or SNMP management application to query the objects in each MIB.

The NIOS appliance allows read-only access to the MIBs. This is equivalent to the Get and Get Next operations in SNMP.

Loading the Infoblox MIBs

If you are using an SNMP manager toolkit with strict dependency checking, you must download the following Infoblox MIBs in the order they are
1. IB-SMI-MIB.txt  
2. IB-TRAP-MIB.txt  
3. IB-PLATFORMONE-MIB.txt  
4. IB-DNSONE-MIB.txt  
5. IB-DHCPOSE-MIB.txt  
6. IB-DNSSERV-MIB.txt  
7. IB-DHCPSERV-MIB.txt  
8. IB-DHCPV6ONE-MIB.txt

In addition, if the SNMP manager toolkit you use requires a different MIB file naming convention, you can rename the MIB files accordingly.

NET-SNMP MIBs

NIOS appliances support NET-SNMP (formerly UCD-SNMP), a collection of applications used to implement the SNMP protocol. The NET-SNMP MIBs provide the top-level infrastructure for the SNMP MIB tree. They define, among other things, the objects in the SNMP traps that the agent sends when the SNMP engine starts and stops. For information about NET-SNMP and the MIB files distributed with NET-SNMP, refer to [http://net-snmp.sourceforge.net/](http://net-snmp.sourceforge.net/).

For SNMP traps to function properly, you must download the following NET-SNMP MIBs directly from [http://net-snmp.sourceforge.net/docs/mibs](http://net-snmp.sourceforge.net/docs/mibs):

- NET-SNMP-MIB
- UCD-SNMP-MIB

**Note:** Ensure that you save the MIBs as text files in the directory to which you save all the other MIB files.

BGP4 MIB

Infoblox supports BGP4 (Border Gateway Protocol) for DNS anycast addressing. BGP is configured to send SNMP traps to neighboring routers, as defined in [RFC4273](https://tools.ietf.org/html/rfc4273). You must enable and configure the SNMP trap receiver on the Grid member for the member to send SNMP traps. For information, see [SNMP MIB Hierarchy](#).

The BGP protocol service is configured to send SNMP queries about BGP runtime data. The information is returned using the following OIDs and definitions:

<table>
<thead>
<tr>
<th>OID</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.15.900.1.1</td>
<td>Number of peers</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.2</td>
<td>Number of active peers</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.3</td>
<td>Number of AS path entries</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.4</td>
<td>Number of BGP community entries</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.5</td>
<td>Total number of prefixes</td>
</tr>
</tbody>
</table>

For each configured BGP peer (a, b, c, d), the information is returned using the following OIDs and definitions:

<table>
<thead>
<tr>
<th>OID</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.2.1.15.900.1.9.a.b.c.d.1</td>
<td>IP address: same as a.b.c.d</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.9.a.b.c.d.2</td>
<td>State: 0=down, 1=up</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.9.a.b.c.d.3</td>
<td>ASN</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.9.a.b.c.d.4</td>
<td>Prefixes</td>
</tr>
<tr>
<td>1.3.6.1.2.1.15.900.1.9.a.b.c.d.5</td>
<td>Up/Down time</td>
</tr>
</tbody>
</table>

ibTrap MIB

NIOS appliances send SNMP traps when events, internal process failures, or critical service failures occur. The ibTrap MIB defines the types of traps that a NIOS appliance sends and the value that each MIB object represents. The Infoblox SNMP traps report objects which the ibTrap MIB defines. Figure 39.3 illustrates the ibTrap MIB structure. It provides the OID and textual description for each object.

**Note:** OIDs shown in the illustrations and tables in this section do not include the prefix .1.3.6.1.4.1.7779.
The ibTrap MIB comprises two trees, ibTrapOneModule and ibNotificationVarBind. The ibTraponeModule tree contains objects for the types of traps that a NIOS appliance sends. The ibNotificationVarBind tree contains objects that the Infoblox SNMP traps report. You cannot send queries for the objects in this MIB module. The objects are used only in the SNMP traps.

**Figure 39.3 ibTrapOne MIB Structure**

![ibTrap One MIB Structure Diagram]

Interpreting Infoblox SNMP Traps

Depending on the SNMP management application your management system uses, the SNMP traps you receive may list the OIDs for all relevant MIB objects from both the ibTrapOneModule and ibNotificationVarBind trees. For OIDs that have string values, the trap lists the text. For OIDs that contain integers, you can use the tables in this section to find out the values. Some SNMP management applications list only the object names and their corresponding values in the SNMP traps. Whether or not your SNMP management application lists OIDs, you can use the tables in this section to find out the corresponding value and definition for each MIB object.

The following is a sample trap a NIOS appliance sends:

```
0:00:10.80 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.7779.3.1.1.1.4.0
SNMPv2-SMI::enterprises.7779.3.1.1.2.1.0 = STRING: "10.35.1.156"
```
The sample trap lists the OIDs and their corresponding values that can help you identify the cause of an event or problem. To identify the possible cause and recommended actions for the trap, use the ibTrapDesc tables. For information, see ibTrapDesc (OID 3.1.1.1.2.11.0).

You can interpret the sample trap as follows:

Using the ibTrapOneModule table, you find out OID 7779.3.1.1.1.4.0 represents an Object State Change trap. This trap includes the following objects: ibNodeName, ibObjectName, ibPreviousState, ibCurrentState, and ibtrapDesc. For each object, the trap displays the OID and its corresponding value. The following is how you can interpret the rest of the trap:

- **ibNodeName (OID 7779.3.1.1.1.2.1.0)**
  - The statement "7779.3.1.1.1.2.1.0 = STRING: "10.35.1.156" SNMPv2-SMI::enterprises.*" tells you the IP address of the appliance on which the trap occurred.

- **ibObjectName (OID 7779.3.1.1.1.2.3.0)**
  - The statement "7779.3.1.1.1.2.3.0 = STRING: "ntp_sync" SNMPv2-SMI::enterprises.*" tells you the MIB object ibObjectName, which is the name of the object for which the trap was generated, has a value of "ntp_sync" that indicates NTP synchronization issues.

- **ibPreviousState (OID 7779.3.1.1.1.2.9.0)**
  - The statement "7779.3.1.1.1.2.9.0 = INTEGER: 15 SNMPv2-SMI::enterprises.*" tells you the MIB object ibPreviousState, which indicates the previous state of the appliance, has a value of 15. Using the ibPreviousState and ibCurrentState Values table, you know that 15 represents "ntp-sync-up", which means the NTP server was up and running.

- **ibCurrentState (OID 7779.3.1.1.1.2.10.0)**
  - The statement "7779.3.1.1.1.2.10.0 = INTEGER: 16 SNMPv2-SMI::enterprises.*" tells you the MIB object ibCurrentState, which indicates the current state of the appliance, has a value of 16. Using the ibPreviousState and ibCurrentState Values table, you know that 16 represents "ntp-sync-down", which means the NTP server is now out of sync.

- **ibTrapDesc (OID 7779.3.1.1.1.2.11.0)**
  - The last statement "7779.3.1.1.1.2.11.0 = STRING: "The NTP service is out of synchronization." states the description of the trap. Using the Object State Change Traps table for ibTrapDesc, you can find out the trap description and recommended actions for this problem.

### Types of Traps (OID 3.1.1.1.1)

ibTrapOneModule defines the types of traps that the NIOS appliance can send. There are five types of SNMP traps. Table 39.4 describes the types of traps and their objects in the ibTrapOneModule tree.

**Note:** Some SNMP traps for ibThresholdCrossingEvent, ibStateChangeEvent, ibProcStartStopTrap, and ibRevokedLicenseTrap do not have an associated ibProbableCause. The following table lists traps that provide ibProbableCause and those that do not have an ibProbableCause value.

#### Table 39.4 ibTrapOneModule

<table>
<thead>
<tr>
<th>Trap Binding Variables (OID 3.1.1.1.2)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OID</strong></td>
</tr>
<tr>
<td>3.1.1.1.1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>3.1.1.1.1.2</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Threshold Crossing

The NIOS appliance generates this trap when any of the following events occur:
- System memory or disk usage exceeds 90%.
- CPU usage exceeds the trigger value for 15 seconds.
- A problem occurs when the Grid Master replicates its database to its Grid members.
- DHCP address usage crosses a watermark threshold. For more information about tracking IP address usage, see Threshold Crossing Traps.
- The number or percentage of the DNS security alerts exceeds the thresholds of the DNS security alert triggers.

This trap includes the following objects:
- ibNodeName
- ibTrapSeverity
- ibObjectName (threshold name)
- ibCurThresholdvalue
- ibThresholdHigh
- ibThresholdLow
- ibTrapDesc

For a list of trap descriptions, see Threshold Crossing Traps.

Object State Change

The NIOS appliance generates this trap when there is a change in its state, such as:
- The link to one of the configured ports goes down, and then goes back up again.
- A failover occurs in an HA (high availability) pair configuration.
- A member connects to the Grid Master.
- An appliance in a Grid goes offline. This trap includes the following objects:
  - ibNodeName
  - ibTrapSeverity
  - ibObjectName
  - ibPreviousState
  - ibCurrentState
  - ibTrapDesc

For a list of possible trap descriptions, see Object State Change Traps.

Process Started and Stopped

The NIOS appliance generates this type of trap when any of the following events occur:
- When you enable HTTP redirection.
- When you change the HTTP access setting.
- When you change the HTTP session time out setting.
- When a failover occurs in an HA pair configuration.

This trap includes the following objects:
- ibNodeName
- ibSubsystemName
- ibTrapDesc

For a list of possible trap descriptions, see Process Started and Stopped Traps.

ibRevokedLicenseTrap

The NIOS appliance generates this trap when a license is revoked. This trap includes the following objects:
- ibNodeName
- ibSubsystemName
- ibTrapDesc

ibOperationTrap

The NIOS appliance generates this trap when a software operation is noteworthy. This trap includes the following objects:
- ibNodeName
- ibTrapSeverity
- ibSubsystemName
- ibProbableCause
- ibTrapDesc

Each SNMP trap contains information about the event or the problem. The Infoblox SNMP traps include MIB objects and their corresponding values from the ibNotificationVarBind module. Table 39.5 describes the objects in the ibNotificationVarBind module.

Table 39.5 ibNotificationVarBind (OID 3.1.1.1.2)

<table>
<thead>
<tr>
<th>OID</th>
<th>MIB Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1.1.2.1.0</td>
<td>ibNodeName (DisplayString)</td>
<td>The IP address of the appliance on which the trap occurs. This may or may not be the same as the appliance that sends the trap. This object is used in all types of traps.</td>
</tr>
<tr>
<td>3.1.1.1.2.2.0</td>
<td>ibTrapSeverity (Integer)</td>
<td>The severity of the trap. There are five levels of severity. See Trap Severity (OID 3.1.1.1.2.2.0) for details.</td>
</tr>
</tbody>
</table>

Note: The OIDs shown in the following table do not include the prefix ".1.3.6.1.4.1.7779.".
3.1.1.2.3.0 ibObjectName (DisplayString)
The name of the object for which the trap was generated. This is used in the Equipment Failure traps, Threshold Crossing Event traps, and the Object State Change traps. The following shows what this object represents depending on the type of traps:
- Equipment Failure traps: The equipment name.
- Threshold Crossing Event traps: The object name of the trap.
- State Change traps: The object that changes state.

3.1.1.2.4.0 ibProbableCause (Integer)
The probable cause of the trap. See ibProbableCause Values for the definitions of each value.

3.1.1.2.5.0 ibSubsystemName (DisplayString)
The subsystem for which the trap was generated, such as NTP or SNMP. This object is used in the Processing and Software Failure traps and the Process Start and Stop traps. See ibSubsystemName Values (OID 3.1.1.1.2.5.0) for definitions.

3.1.1.2.6.0 ibCurThresholdValue (Integer)
The current value of the threshold counter. This object is used in the Threshold Crossing traps.

3.1.1.2.7.0 ibThresholdHigh (Integer)
This object is used in Threshold Crossing traps. For CPU usage, this is the trigger value of the SNMP trap. For DHCP address usage, this is the value of the high watermark. This only applies when the appliance sends a trap to indicate that DHCP address usage is above the configured high watermark value for a DHCP address range. For more information, see Threshold Crossing Traps.

3.1.1.2.8.0 ibThresholdLow (Integer)
This object is used in Threshold Crossing traps. For CPU usage, this is the reset value of the SNMP trap. For DHCP address usage, this is the value for the low watermark. This only applies when the appliance sends a trap to indicate that DHCP address usage went below the configured low watermark value for a DHCP address range. For more information, see Threshold Crossing Traps.

3.1.1.2.9.0 ibPreviousState (Integer)
The previous state of the appliance. This object is used in the Object State Change traps. See ibPreviousState (OID 3.1.1.1.2.9.0) and ibCurrentState (OID 3.1.1.1.2.10.0) for definitions of each value.

3.1.1.2.10.0 ibCurrentState (Integer)
The current state of the appliance. This object is used in the Object State Change traps. See ibPreviousState (OID 3.1.1.1.2.9.0) and ibCurrentState (OID 3.1.1.1.2.10.0) for the definition of each value.

3.1.1.2.11.0 ibTrapDesc (DisplayString)
The description of the trap. This object is used in all types of traps. See ibTrapDesc (OID 3.1.1.1.2.11.0) for the description, possible cause, and recommended actions for each Infoblox SNMP trap.

### Trap Severity (OID 3.1.1.1.2.2.0)
The object ibTrapSeverity defines the severity level for each Infoblox SNMP trap. There are five levels of severity.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Indetermined [sic]</td>
</tr>
<tr>
<td>2</td>
<td>Informational: Event that requires no further action.</td>
</tr>
<tr>
<td>3</td>
<td>Minor: Event that does not require user intervention.</td>
</tr>
<tr>
<td>4</td>
<td>Major: Event that requires user intervention and assistance from Infoblox Technical Support.</td>
</tr>
<tr>
<td>5</td>
<td>Critical: Problem that affects services and system operations, and requires assistance from Infoblox Technical Support.</td>
</tr>
</tbody>
</table>

### ibProbableCause Values (OID 3.1.1.1.2.4.0)
Table 39.6 lists the values that are associated with the object ibProbableCause (OID 3.1.1.1.2.4.0). These values provide information about the events such as hardware, software for process failures, that trigger SNMP traps.

Table 39.6 ibProbableCause Values

<table>
<thead>
<tr>
<th>Value</th>
<th>OID 3.1.1.2.4.0 ibProbableCause</th>
<th>Equipment, Software, or Process Failure Traps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright ©2019, Infoblox, Inc.All right reserved.
<table>
<thead>
<tr>
<th>Code</th>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ibClear</td>
<td>SNMP Trap is cleared.</td>
</tr>
<tr>
<td>1</td>
<td>ibUnknown</td>
<td>An unknown failure has occurred.</td>
</tr>
<tr>
<td>2</td>
<td>ibPrimaryDiskFailure</td>
<td>A primary drive failure has occurred.</td>
</tr>
<tr>
<td>3</td>
<td>ibFanFailure-old</td>
<td>Unused.</td>
</tr>
<tr>
<td>4</td>
<td>ibPowerSupplyFailure</td>
<td>A power supply failure has occurred.</td>
</tr>
<tr>
<td>5</td>
<td>ibDBFailure</td>
<td>A database daemon monitoring failure has occurred.</td>
</tr>
<tr>
<td>6</td>
<td>ibApacheSoftwareFailure</td>
<td>An apache software failure has occurred.</td>
</tr>
<tr>
<td>7</td>
<td>ibSerialConsoleFailure</td>
<td>An Infoblox serial console software failure has occurred.</td>
</tr>
<tr>
<td>11</td>
<td>ibControldSoftwareFailure</td>
<td>A controld failure has occurred.</td>
</tr>
<tr>
<td>12</td>
<td>ibUpgradeFailure</td>
<td>A system upgrade failure has occurred.</td>
</tr>
<tr>
<td>13</td>
<td>ibSNMPDFailure</td>
<td>SNMP Server failure has occurred.</td>
</tr>
<tr>
<td>15</td>
<td>ibSSHDSoftwareFailure</td>
<td>An SSH daemon failure has occurred.</td>
</tr>
<tr>
<td>16</td>
<td>ibNTPDSoftwareFailure</td>
<td>An NTP daemon failure has occurred.</td>
</tr>
<tr>
<td>17</td>
<td>ibClusterdSoftwareFailure</td>
<td>A cluster daemon failure has occurred.</td>
</tr>
<tr>
<td>18</td>
<td>ibLCDSoftwareFailure</td>
<td>An LCD daemon failure has occurred.</td>
</tr>
<tr>
<td>19</td>
<td>ibDHCPdSoftwareFailure</td>
<td>A DHCP daemon monitoring failure has occurred.</td>
</tr>
<tr>
<td>20</td>
<td>ibNamedSoftwareFailure</td>
<td>A named daemon monitoring failure has occurred.</td>
</tr>
<tr>
<td>21</td>
<td>ibAuthServerGroupDown</td>
<td>NAC Authentication server group is down.</td>
</tr>
<tr>
<td>22</td>
<td>ibAuthServerGroupUp</td>
<td>NAC Authentication server group is up.</td>
</tr>
<tr>
<td>24</td>
<td>ibNTLMSoftwareFailure</td>
<td>An NTLM monitoring failure has occurred.</td>
</tr>
<tr>
<td>25</td>
<td>ibNetBIOSDaemonFailure</td>
<td>A NetBIOS daemon monitoring failure has occurred.</td>
</tr>
<tr>
<td>26</td>
<td>ibWindowBindDaemonFailure</td>
<td>An NT domain service monitoring failure has occurred.</td>
</tr>
<tr>
<td>27</td>
<td>ibTFTPDSoftwareFailure</td>
<td>A TFTPD daemon failure has occurred.</td>
</tr>
<tr>
<td>28</td>
<td>ibUNUSED28</td>
<td>Unused.</td>
</tr>
<tr>
<td>29</td>
<td>ibBackupSoftwareFailure</td>
<td>Backup failed.</td>
</tr>
<tr>
<td>30</td>
<td>ibBackupDatabaseSoftwareFailure</td>
<td>Database backup failed.</td>
</tr>
<tr>
<td>31</td>
<td>ibBackupModuleSoftwareFailure</td>
<td>Module backup failed.</td>
</tr>
<tr>
<td>32</td>
<td>ibBackupSizeSoftwareFailure</td>
<td>File size exceeded the quota. Backup failed.</td>
</tr>
<tr>
<td>33</td>
<td>ibBackupLockSoftwareFailure</td>
<td>Another backup is in progress. Backup will not be performed.</td>
</tr>
<tr>
<td>34</td>
<td>ibHTTPFileDistSoftwareFailure</td>
<td>An HTTP file distribution daemon failure has occurred.</td>
</tr>
<tr>
<td>35</td>
<td>ibOSPFSoftwareFailure</td>
<td>An OSPF routing daemon failure has occurred.</td>
</tr>
<tr>
<td>36</td>
<td>ibAuthDHCPNamedSoftwareFailure</td>
<td>An auth named server failure has occurred.</td>
</tr>
<tr>
<td>37</td>
<td>ibFan1Failure</td>
<td>Fan 1 failure has occurred.</td>
</tr>
<tr>
<td>Line</td>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>38</td>
<td>ibFan2Failure</td>
<td>Fan 2 failure has occurred.</td>
</tr>
<tr>
<td>39</td>
<td>ibFan3Failure</td>
<td>Fan 3 failure has occurred.</td>
</tr>
<tr>
<td>40</td>
<td>ibFan1OK</td>
<td>Fan 1 is OK.</td>
</tr>
<tr>
<td>41</td>
<td>ibFan2OK</td>
<td>Fan 2 is OK.</td>
</tr>
<tr>
<td>42</td>
<td>ibFan3OK</td>
<td>Fan 3 is OK.</td>
</tr>
<tr>
<td>44</td>
<td>ibFTPDSoftwareFailure</td>
<td>An FTPD daemon failure has occurred.</td>
</tr>
<tr>
<td>45</td>
<td>ibBloxtoolsSoftwareFailure</td>
<td>A Bloxtools service failure has occurred.</td>
</tr>
<tr>
<td>46</td>
<td>ibPowerSupplyOK</td>
<td>The power supply is OK.</td>
</tr>
<tr>
<td>47</td>
<td>ibWebUISoftwareFailure</td>
<td>A WebUI software failure has occurred.</td>
</tr>
<tr>
<td>48</td>
<td>ibUNUSED48</td>
<td>Unused.</td>
</tr>
<tr>
<td>49</td>
<td>ibADAgentSyncFailure</td>
<td>An AD agent client synchronizing domain data failure has occurred.</td>
</tr>
<tr>
<td>50</td>
<td>ibIFMAPSoftwareFailure</td>
<td>An IF-MAP server failure has occurred.</td>
</tr>
<tr>
<td>51</td>
<td>ibCaptivePortalSoftwareFailure</td>
<td>A Captive Portal service failure has occurred.</td>
</tr>
<tr>
<td>52</td>
<td>ibDuplicateIPAddressFailure</td>
<td>A Duplicate IP Address has been detected.</td>
</tr>
<tr>
<td>53</td>
<td>ibBGPSoftwareFailure</td>
<td>An BGP routing daemon failure has occurred.</td>
</tr>
<tr>
<td>54</td>
<td>ibRevokedLicense</td>
<td>A license has been revoked.</td>
</tr>
<tr>
<td>58</td>
<td>ibGUILoginFailure</td>
<td>An admin failed to log in to the GUI.</td>
</tr>
<tr>
<td>59</td>
<td>ibSerialConsoleLoginFailure</td>
<td>An admin failed to log in to the serial console.</td>
</tr>
<tr>
<td>60</td>
<td>ibSystemReboot</td>
<td>A system reboot was initiated.</td>
</tr>
<tr>
<td>61</td>
<td>ibSystemRestart</td>
<td>A system restart was initiated.</td>
</tr>
<tr>
<td>62</td>
<td>ibZoneTransferFailure</td>
<td>A zone transfer failure occurred.</td>
</tr>
<tr>
<td>63</td>
<td>ibDHCPLeaseConflict</td>
<td>DHCP address conflicts with an existing lease.</td>
</tr>
<tr>
<td>64</td>
<td>ibDHCPAddressConflict</td>
<td>DHCP address conflicts with an existing fixed address.</td>
</tr>
<tr>
<td>65</td>
<td>ibDHCPRangeConflict</td>
<td>DHCP address conflicts with an existing range.</td>
</tr>
<tr>
<td>66</td>
<td>ibDHCPHostConflict</td>
<td>DHCP address conflicts with an existing host.</td>
</tr>
<tr>
<td>67</td>
<td>ibSyslogFailure</td>
<td>A syslog daemon failure occurred.</td>
</tr>
<tr>
<td>68</td>
<td>ibPowerSupply1Failure</td>
<td>Power supply 1 failure has occurred.</td>
</tr>
<tr>
<td>69</td>
<td>ibPowerSupply2Failure</td>
<td>Power supply 2 failure has occurred.</td>
</tr>
<tr>
<td>70</td>
<td>ibPowerSupply1OK</td>
<td>Power supply 1 is OK.</td>
</tr>
<tr>
<td>71</td>
<td>ibPowerSupply2OK</td>
<td>Power supply 2 is OK.</td>
</tr>
<tr>
<td>72</td>
<td>ibReportingTaskSwFailure</td>
<td>A reporting task monitoring failure has occurred.</td>
</tr>
<tr>
<td>73</td>
<td>ibReportingDbBackupFailure</td>
<td>A reporting db backup/restore operation failure has occurred.</td>
</tr>
<tr>
<td>74</td>
<td>ibFan4Failure</td>
<td>Fan 4 failure has occurred.</td>
</tr>
<tr>
<td>75</td>
<td>ibFan5Failure</td>
<td>Fan 5 failure has occurred.</td>
</tr>
<tr>
<td>Line</td>
<td>Event Description</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>76</td>
<td>ibFan6Failure</td>
<td>Fan 6 failure has occurred.</td>
</tr>
<tr>
<td>77</td>
<td>ibFan7Failure</td>
<td>Fan 7 failure has occurred.</td>
</tr>
<tr>
<td>78</td>
<td>ibFan8Failure</td>
<td>Fan 8 failure has occurred.</td>
</tr>
<tr>
<td>79</td>
<td>ibFan4OK</td>
<td>Fan 4 is OK.</td>
</tr>
<tr>
<td>80</td>
<td>ibFan5OK</td>
<td>Fan 5 is OK.</td>
</tr>
<tr>
<td>81</td>
<td>ibFan6OK</td>
<td>Fan 6 is OK.</td>
</tr>
<tr>
<td>82</td>
<td>ibFan7OK</td>
<td>Fan 7 is OK.</td>
</tr>
<tr>
<td>83</td>
<td>ibFan8OK</td>
<td>Fan 8 is OK.</td>
</tr>
<tr>
<td>84</td>
<td>ibOSPF6SoftwareFailure</td>
<td>An OSPF6 routing daemon failure has occurred.</td>
</tr>
<tr>
<td>85</td>
<td>ibOCSPResponderFailure</td>
<td>OCSP responder failed.</td>
</tr>
<tr>
<td>86</td>
<td>ibReportingAlertTriggered</td>
<td>A reporting alert is triggered.</td>
</tr>
<tr>
<td>87</td>
<td>ibCapturedQueriesUploadFailure</td>
<td>Upload for captured DNS queries failed.</td>
</tr>
<tr>
<td>88</td>
<td>ibLDAPServerFailure</td>
<td>The LDAP server failed.</td>
</tr>
<tr>
<td>89</td>
<td>ibRIRWIPRegistrationFailure</td>
<td>RIR SWIP registration failed.</td>
</tr>
<tr>
<td>90</td>
<td>ibPowerSupply1Removed</td>
<td>Power supply 1 has been removed.</td>
</tr>
<tr>
<td>91</td>
<td>ibPowerSupply2Removed</td>
<td>Power supply 2 has been removed.</td>
</tr>
<tr>
<td>92</td>
<td>ibIPMISensorErrorDetected</td>
<td>Error detected on the sensor for the IPMI port (used for LOM)</td>
</tr>
<tr>
<td>93</td>
<td>ibDiscoveryConsolidatorTaskSwFailure</td>
<td>Discovery service on the Consolidator failed.</td>
</tr>
<tr>
<td>94</td>
<td>ibDiscoveryCollectorTaskSwFailure</td>
<td>Discovery service on probes failed.</td>
</tr>
<tr>
<td>95</td>
<td>ibDiscoveryBackupSwFailure</td>
<td>Discovery backup service failed.</td>
</tr>
<tr>
<td>96</td>
<td>ibThreatProtectionAutoDownloadFailure</td>
<td>Automatic download of threat protection rule failed.</td>
</tr>
<tr>
<td>97</td>
<td>ibThreatProtectionPublishFailure</td>
<td>Threat protection rule publish failed.</td>
</tr>
<tr>
<td>98</td>
<td>ibPassiveHANodeARPConnectivityFailure</td>
<td>HA node failed to connect to local router.</td>
</tr>
<tr>
<td>99</td>
<td>ibPassiveHANodeARPConnectivitySuccess</td>
<td>HA node successfully connects to local router.</td>
</tr>
<tr>
<td>100</td>
<td>ibDNSIntegrityCheckConnectionFailed</td>
<td>Connection between Grid member and Grid Master failed.</td>
</tr>
<tr>
<td>101</td>
<td>ibDNSIntegrityCheckPrimaryServersFailed</td>
<td>DNS data (NS RRset) check for Grid primaries failed.</td>
</tr>
<tr>
<td>102</td>
<td>ibDNSIntegrityCheckNameserversFailed</td>
<td>DNS data (NS RRset) check for name servers failed.</td>
</tr>
<tr>
<td>103</td>
<td>ibCloudAPIFailure</td>
<td>Cloud API service failed.</td>
</tr>
<tr>
<td>104</td>
<td>ibRpzRefreshFailure</td>
<td>An RPZ refresh failure has occurred.</td>
</tr>
<tr>
<td>105</td>
<td>ibUnboundSoftwareFailure</td>
<td>Unbound software failure has occurred.</td>
</tr>
<tr>
<td>106</td>
<td>ibAnalyticsAutoDownloadFailure</td>
<td>Automatic download of analytic module set failed.</td>
</tr>
<tr>
<td>107</td>
<td>ibDnsHealthCheckFailed</td>
<td>The DNS health check has failed.</td>
</tr>
<tr>
<td>108</td>
<td>ibDnsHealthCheckSucceed</td>
<td>The DNS health check is successful.</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td>Message</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>109</td>
<td>ibBFDSoftwareFailure</td>
<td>BFD has failed to detect failure in the bidirectional path between two interfaces.</td>
</tr>
<tr>
<td>110</td>
<td>ibOutboundWorkerFailed</td>
<td>An Outbound worker has failed.</td>
</tr>
<tr>
<td>3001</td>
<td>ibRAIDIsOptimal</td>
<td>The system’s RAID array is now running in an optimal state.</td>
</tr>
<tr>
<td>3002</td>
<td>ibRAIDIsDegraded</td>
<td>The system’s RAID array is in a degraded state.</td>
</tr>
<tr>
<td>3003</td>
<td>ibRAIDIsRebuilding</td>
<td>The system’s RAID array is rebuilding.</td>
</tr>
<tr>
<td>3004</td>
<td>ibRAIDStatusUnknown</td>
<td>Unable to retrieve RAID array state!</td>
</tr>
<tr>
<td>3005</td>
<td>ibRAIDBatteryIsOK</td>
<td>The system’s RAID battery is OK.</td>
</tr>
<tr>
<td>3006</td>
<td>ibRAIDBatteryFailed</td>
<td>A RAID battery failure has occurred.</td>
</tr>
<tr>
<td>3007</td>
<td>ibRAIDOptimalMismatch</td>
<td>The system’s RAID array is now running in an optimal state (Mismatched disk(s) found).</td>
</tr>
<tr>
<td>3008</td>
<td>ibRAIDDegradedMismatch</td>
<td>The system’s RAID array is in a degraded state (Mismatched disk(s) found).</td>
</tr>
<tr>
<td>3009</td>
<td>ibRAIDRebuildingMismatch</td>
<td>The system’s RAID array is rebuilding (Mismatched disk(s) found).</td>
</tr>
<tr>
<td>3010</td>
<td>ibRAIDBatteryWeak</td>
<td>Please replace the system’s RAID battery soon.</td>
</tr>
<tr>
<td>3011</td>
<td>ibRAIDIsDegradedDisk1</td>
<td>The system’s RAID array is in a degraded state. RAID Disk1 is EMPTY.</td>
</tr>
<tr>
<td>3012</td>
<td>ibRAIDIsDegradedDisk2</td>
<td>The system’s RAID array is in a degraded state. RAID Disk2 is EMPTY.</td>
</tr>
<tr>
<td>3013</td>
<td>ibRAIDIsDegradedDisk3</td>
<td>The system’s RAID array is in a degraded state. RAID Disk3 is EMPTY.</td>
</tr>
<tr>
<td>3014</td>
<td>ibRAIDIsDegradedDisk4</td>
<td>The system’s RAID array is in a degraded state. RAID Disk4 is EMPTY.</td>
</tr>
<tr>
<td>3015</td>
<td>ibRAIDIsDegradedDisk5</td>
<td>The system’s RAID array is in a degraded state. RAID Disk5 is EMPTY.</td>
</tr>
<tr>
<td>3016</td>
<td>ibRAIDIsDegradedDisk6</td>
<td>The system’s RAID array is in a degraded state. RAID Disk6 is EMPTY.</td>
</tr>
<tr>
<td>3017</td>
<td>ibRAIDIsDegradedDisk7</td>
<td>The system’s RAID array is in a degraded state. RAID Disk7 is EMPTY.</td>
</tr>
<tr>
<td>3018</td>
<td>ibRAIDIsDegradedDisk8</td>
<td>The system’s RAID array is in a degraded state. RAID Disk8 is EMPTY.</td>
</tr>
<tr>
<td>3019</td>
<td>ibRAIDIsRebuildingDisk1</td>
<td>The system’s RAID array is rebuilding. RAID Disk1 is OFFLINE.</td>
</tr>
<tr>
<td>3020</td>
<td>ibRAIDIsRebuildingDisk2</td>
<td>The system’s RAID array is rebuilding. RAID Disk2 is OFFLINE.</td>
</tr>
<tr>
<td>3021</td>
<td>ibRAIDIsRebuildingDisk3</td>
<td>The system’s RAID array is rebuilding. RAID Disk3 is OFFLINE.</td>
</tr>
<tr>
<td>3022</td>
<td>ibRAIDIsRebuildingDisk4</td>
<td>The system’s RAID array is rebuilding. RAID Disk4 is OFFLINE.</td>
</tr>
<tr>
<td>3023</td>
<td>ibRAIDIsRebuildingDisk5</td>
<td>The system’s RAID array is rebuilding. RAID Disk5 is OFFLINE.</td>
</tr>
<tr>
<td>3024</td>
<td>ibRAIDIsRebuildingDisk6</td>
<td>The system’s RAID array is rebuilding. RAID Disk6 is OFFLINE.</td>
</tr>
<tr>
<td>Code</td>
<td>Event</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3025</td>
<td>ibRAIDIsRebuildingDisk7</td>
<td>The system’s RAID array is rebuilding. RAID Disk7 is OFFLINE.</td>
</tr>
<tr>
<td>3026</td>
<td>ibRAIDIsRebuildingDisk8</td>
<td>The system’s RAID array is rebuilding. RAID Disk8 is OFFLINE.</td>
</tr>
<tr>
<td>3027</td>
<td>ibRAIDDegradedMismatchDisk1</td>
<td>The system’s RAID array is in a degraded state (Mismatched disk(s) found). RAID Disk1 is EMPTY.</td>
</tr>
<tr>
<td>3028</td>
<td>ibRAIDDegradedMismatchDisk2</td>
<td>The system’s RAID array is in a degraded state (Mismatched disk(s) found). RAID Disk2 is EMPTY.</td>
</tr>
<tr>
<td>3029</td>
<td>ibRAIDDegradedMismatchDisk3</td>
<td>The system’s RAID array is in a degraded state (Mismatched disk(s) found). RAID Disk3 is EMPTY.</td>
</tr>
<tr>
<td>3030</td>
<td>ibRAIDDegradedMismatchDisk4</td>
<td>The system’s RAID array is in a degraded state (Mismatched disk(s) found). RAID Disk4 is EMPTY.</td>
</tr>
<tr>
<td>3031</td>
<td>ibRAIDDegradedMismatchDisk5</td>
<td>The system’s RAID array is in a degraded state (Mismatched disk(s) found). RAID Disk5 is EMPTY.</td>
</tr>
<tr>
<td>3032</td>
<td>ibRAIDDegradedMismatchDisk6</td>
<td>The system’s RAID array is in a degraded state (Mismatched disk(s) found). RAID Disk6 is EMPTY.</td>
</tr>
<tr>
<td>3033</td>
<td>ibRAIDDegradedMismatchDisk7</td>
<td>The system’s RAID array is in a degraded state (Mismatched disk(s) found). RAID Disk7 is EMPTY.</td>
</tr>
<tr>
<td>3034</td>
<td>ibRAIDDegradedMismatchDisk8</td>
<td>The system’s RAID array is in a degraded state (Mismatched disk(s) found). RAID Disk8 is EMPTY.</td>
</tr>
<tr>
<td>3035</td>
<td>ibRAIDRebuildingMismatchDisk1</td>
<td>The system’s RAID array is rebuilding (Mismatched disk(s) found). RAID Disk1 is OFFLINE.</td>
</tr>
<tr>
<td>3036</td>
<td>ibRAIDRebuildingMismatchDisk2</td>
<td>The system’s RAID array is rebuilding (Mismatched disk(s) found). RAID Disk2 is OFFLINE.</td>
</tr>
<tr>
<td>3037</td>
<td>ibRAIDRebuildingMismatchDisk3</td>
<td>The system’s RAID array is rebuilding (Mismatched disk(s) found). RAID Disk3 is OFFLINE.</td>
</tr>
<tr>
<td>3038</td>
<td>ibRAIDRebuildingMismatchDisk4</td>
<td>The system’s RAID array is rebuilding (Mismatched disk(s) found). RAID Disk4 is OFFLINE.</td>
</tr>
<tr>
<td>3039</td>
<td>ibRAIDRebuildingMismatchDisk5</td>
<td>The system’s RAID array is rebuilding (Mismatched disk(s) found). RAID Disk5 is OFFLINE.</td>
</tr>
<tr>
<td>3040</td>
<td>ibRAIDRebuildingMismatchDisk6</td>
<td>The system’s RAID array is rebuilding (Mismatched disk(s) found). RAID Disk6 is OFFLINE.</td>
</tr>
<tr>
<td>3041</td>
<td>ibRAIDRebuildingMismatchDisk7</td>
<td>The system’s RAID array is rebuilding (Mismatched disk(s) found). RAID Disk7 is OFFLINE.</td>
</tr>
<tr>
<td>3042</td>
<td>ibRAIDRebuildingMismatchDisk8</td>
<td>The system’s RAID array is rebuilding (Mismatched disk(s) found). RAID Disk8 is OFFLINE.</td>
</tr>
<tr>
<td>3043</td>
<td>ibRAIDIsInoperative</td>
<td>The system’s RAID array is inoperative.</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>4001</td>
<td>ibDisconnectGridAttachFailed</td>
<td></td>
</tr>
<tr>
<td>4002</td>
<td>ibDisconnectedGridDetachFailed</td>
<td></td>
</tr>
<tr>
<td>4003</td>
<td>ibDisconnectedGridDetachFailedSubgrid Offline</td>
<td></td>
</tr>
<tr>
<td>4004</td>
<td>ibDisconnectedGridSnapshotFailed</td>
<td></td>
</tr>
<tr>
<td>4005</td>
<td>ibDnssecAutomaticKSKRolloverApproching</td>
<td></td>
</tr>
<tr>
<td>4006</td>
<td>ibDnssecManualKSKRolloverDueApproaching</td>
<td></td>
</tr>
<tr>
<td>4007</td>
<td>ibDnssecAutomaticKSKRolloverDone</td>
<td></td>
</tr>
<tr>
<td>4008</td>
<td>ibDnssecManualKSKRolloverDone</td>
<td></td>
</tr>
<tr>
<td>4009</td>
<td>ibDnssecKSKRolloverOverdue</td>
<td></td>
</tr>
<tr>
<td>4010</td>
<td>ibPortDiscoveryConflict</td>
<td></td>
</tr>
<tr>
<td>4011</td>
<td>ibDeviceDiscoveryConflict</td>
<td></td>
</tr>
<tr>
<td>4012</td>
<td>ibDeviceUnmanaged</td>
<td></td>
</tr>
<tr>
<td>4013</td>
<td>ibAnalyticsDnstUpdate</td>
<td></td>
</tr>
<tr>
<td>4014</td>
<td>ibSyslogBackupDone</td>
<td></td>
</tr>
<tr>
<td>4015</td>
<td>ibSyslogBackupFailed</td>
<td></td>
</tr>
</tbody>
</table>

**ibSubsystemName Values (OID 3.1.1.1.2.5.0)**

Table 39.7 lists the values that are associated with the object `ibSubsystemName` (OID 3.1.1.1.2.5.0). These values provide information about the subsystems that trigger the traps.

<table>
<thead>
<tr>
<th>Value</th>
<th>OID 3.1.1.1.2.5.0 <code>ibSubsystemName</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Uses the original <code>ibObjectName</code> and <code>ibSubsystemName</code> when the trap is cleared. The process failure trap is appended to the CLEAR trap descriptions.</td>
</tr>
<tr>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>N/A</td>
</tr>
<tr>
<td>4</td>
<td>N/A</td>
</tr>
<tr>
<td>5</td>
<td>Db_jnld</td>
</tr>
<tr>
<td>6</td>
<td>httpd</td>
</tr>
<tr>
<td>7</td>
<td>serial_console</td>
</tr>
<tr>
<td>11</td>
<td>controld</td>
</tr>
<tr>
<td>12</td>
<td>N/A</td>
</tr>
<tr>
<td>13</td>
<td>Snmpd</td>
</tr>
<tr>
<td>15</td>
<td>Sshd</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>16</td>
<td>Ntpd</td>
</tr>
<tr>
<td>17</td>
<td>Clusterd</td>
</tr>
<tr>
<td>18</td>
<td>Lcd</td>
</tr>
<tr>
<td>19</td>
<td>Dhcpd</td>
</tr>
<tr>
<td>20</td>
<td>Named</td>
</tr>
<tr>
<td>24</td>
<td>NTLM</td>
</tr>
<tr>
<td>25</td>
<td>Netbiosd</td>
</tr>
<tr>
<td>26</td>
<td>Winbindd</td>
</tr>
<tr>
<td>27</td>
<td>Tftpd</td>
</tr>
<tr>
<td>29</td>
<td>N/A</td>
</tr>
<tr>
<td>30</td>
<td>db_dump</td>
</tr>
<tr>
<td>31</td>
<td>N/A</td>
</tr>
<tr>
<td>32</td>
<td>Scheduled_backups</td>
</tr>
<tr>
<td>33</td>
<td>N/A</td>
</tr>
<tr>
<td>34</td>
<td>HTTPd</td>
</tr>
<tr>
<td>35</td>
<td>OSPF</td>
</tr>
<tr>
<td>36</td>
<td>AuthDhcpNamed</td>
</tr>
<tr>
<td>44</td>
<td>ftpd</td>
</tr>
<tr>
<td>45</td>
<td>bloxtools</td>
</tr>
<tr>
<td>47</td>
<td>webui</td>
</tr>
<tr>
<td>50</td>
<td>imap</td>
</tr>
<tr>
<td>51</td>
<td>captive_portal</td>
</tr>
<tr>
<td>53</td>
<td>BGP</td>
</tr>
<tr>
<td>58</td>
<td>GUI_Login</td>
</tr>
<tr>
<td>72</td>
<td>Reporting_task</td>
</tr>
<tr>
<td>84</td>
<td>OSPF6</td>
</tr>
<tr>
<td>95</td>
<td>Discovery_backups</td>
</tr>
<tr>
<td>105</td>
<td>Unbounds</td>
</tr>
<tr>
<td></td>
<td>- HA_Replication</td>
</tr>
<tr>
<td></td>
<td>- HSM Group Status</td>
</tr>
<tr>
<td></td>
<td>- Cluster</td>
</tr>
<tr>
<td></td>
<td>- Cluster_Send_Queue</td>
</tr>
<tr>
<td></td>
<td>- Cluster_Recv_Queue</td>
</tr>
<tr>
<td></td>
<td>- RPZHITRate</td>
</tr>
<tr>
<td></td>
<td>- Authentication Server Group</td>
</tr>
</tbody>
</table>

**ibPreviousState (OID 3.1.1.2.9.0) and ibCurrentState (OID 3.1.1.2.10.0)**

The ibPreviousState object indicates the state of the appliance before the event triggered the trap. The ibCurrentState object indicates the current
Table 39.8 shows the message and description for each state.

Table 39.8 ibPreviousState and IbCurrentState Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ha-active</td>
<td>The HA pair is in ACTIVE state.</td>
</tr>
<tr>
<td>2</td>
<td>ha-passive</td>
<td>The HA pair is in PASSIVE state.</td>
</tr>
<tr>
<td>3</td>
<td>ha-initial</td>
<td>The HA pair is in INITIAL state.</td>
</tr>
<tr>
<td>4</td>
<td>Grid-connected</td>
<td>The Grid member is connected to the Grid Master.</td>
</tr>
<tr>
<td>5</td>
<td>Grid-disconnected</td>
<td>The Grid member is not connected to the Grid Master.</td>
</tr>
<tr>
<td>6</td>
<td>enet-link-up</td>
<td>The ethernet port link is active.</td>
</tr>
<tr>
<td>7</td>
<td>enet-link-down</td>
<td>The ethernet port link is inactive.</td>
</tr>
<tr>
<td>8</td>
<td>replication-online</td>
<td>The replication is online.</td>
</tr>
<tr>
<td>9</td>
<td>replication-offline</td>
<td>The replication is offline.</td>
</tr>
<tr>
<td>10</td>
<td>replication-snapshotting</td>
<td>The replication is snapshotting.</td>
</tr>
<tr>
<td>11</td>
<td>service-up</td>
<td>The service is up.</td>
</tr>
<tr>
<td>12</td>
<td>service-down</td>
<td>The service is down.</td>
</tr>
<tr>
<td>13</td>
<td>ha-replication-online</td>
<td>The HA pair replication is online.</td>
</tr>
<tr>
<td>14</td>
<td>ha-replication-offline</td>
<td>The HA pair replication is offline.</td>
</tr>
<tr>
<td>15</td>
<td>ntp-syn-up</td>
<td>The NTP server is synchronizing.</td>
</tr>
<tr>
<td>16</td>
<td>ntp-syn-down</td>
<td>The NTP server is out of synchronization.</td>
</tr>
<tr>
<td>17</td>
<td>ms-server-up</td>
<td>Microsoft server is up.</td>
</tr>
<tr>
<td>18</td>
<td>ms-server-down</td>
<td>Microsoft server is down.</td>
</tr>
<tr>
<td>19</td>
<td>ms-service-up</td>
<td>Microsoft service connection is active.</td>
</tr>
<tr>
<td>20</td>
<td>ms-service-down</td>
<td>Microsoft service connection is inactive.</td>
</tr>
<tr>
<td>21</td>
<td>nac-server-group-down</td>
<td>NAC Authentication server group is down.</td>
</tr>
<tr>
<td>22</td>
<td>nac-server-group-up</td>
<td>NAC Authentication server group is up.</td>
</tr>
<tr>
<td>23</td>
<td>mgm-service-up</td>
<td>MGM service is active.</td>
</tr>
<tr>
<td>24</td>
<td>mgm-service-down</td>
<td>MGM service is inactive.</td>
</tr>
<tr>
<td>25</td>
<td>ha-active-active</td>
<td>HA Pair is in Dual Active state.</td>
</tr>
<tr>
<td>26</td>
<td>ftp-service-working</td>
<td>FTP service is working.</td>
</tr>
<tr>
<td>27</td>
<td>ftp-service-failed</td>
<td>FTP service failed.</td>
</tr>
<tr>
<td>28</td>
<td>ftp-service-inactive</td>
<td>FTP service is inactive.</td>
</tr>
<tr>
<td>29</td>
<td>tftp-service-working</td>
<td>TFTP service is working.</td>
</tr>
<tr>
<td>30</td>
<td>tftp-service-failed</td>
<td>TFTP service failed.</td>
</tr>
<tr>
<td>31</td>
<td>tftp-service-inactive</td>
<td>TFTP service is inactive.</td>
</tr>
<tr>
<td>32</td>
<td>dns-service-working</td>
<td>DNS service is working.</td>
</tr>
<tr>
<td>33</td>
<td>dns-service-failed</td>
<td>DNS service failed.</td>
</tr>
<tr>
<td>34</td>
<td>dns-service-inactive</td>
<td>DNS service is inactive.</td>
</tr>
<tr>
<td>35</td>
<td>ntp-service-working</td>
<td>NTP service is working.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>36</td>
<td>ntp-service-failed</td>
<td>NTP service failed.</td>
</tr>
<tr>
<td>37</td>
<td>ntp-service-inactive</td>
<td>NTP service is inactive.</td>
</tr>
<tr>
<td>38</td>
<td>http-file-dist-service-working</td>
<td>HTTP File Dist service is working.</td>
</tr>
<tr>
<td>40</td>
<td>http-file-dist-service-inactive</td>
<td>HTTP File Dist service is inactive.</td>
</tr>
<tr>
<td>41</td>
<td>bloxtools-service-working</td>
<td>bloxTools service is working.</td>
</tr>
<tr>
<td>42</td>
<td>bloxtools-service-warning</td>
<td>bloxTools service is in warning state.</td>
</tr>
<tr>
<td>43</td>
<td>bloxtools-service-failed</td>
<td>bloxTools service failed.</td>
</tr>
<tr>
<td>44</td>
<td>bloxtools-service-inactive</td>
<td>bloxTools service is inactive.</td>
</tr>
<tr>
<td>45</td>
<td>dhcp-service-working</td>
<td>DHCP service is working.</td>
</tr>
<tr>
<td>46</td>
<td>dhcp-service-warning</td>
<td>DHCP service is in warning state.</td>
</tr>
<tr>
<td>47</td>
<td>dhcp-service-failed</td>
<td>DHCP service failed.</td>
</tr>
<tr>
<td>48</td>
<td>dhcp-service-inactive</td>
<td>DHCP service is inactive.</td>
</tr>
<tr>
<td>49</td>
<td>captive-portal-service-working</td>
<td>Captive portal service is working.</td>
</tr>
<tr>
<td>50</td>
<td>captive-portal-service-failed</td>
<td>Captive portal service failed.</td>
</tr>
<tr>
<td>51</td>
<td>captive-portal-service-inactive</td>
<td>Captive portal service inactive.</td>
</tr>
<tr>
<td>52</td>
<td>ifmap-service-working</td>
<td>IF-MAP service is working.</td>
</tr>
<tr>
<td>53</td>
<td>ifmap-service-failed</td>
<td>IF-MAP service failed.</td>
</tr>
<tr>
<td>54</td>
<td>ifmap-service-inactive</td>
<td>IF-MAP service inactive.</td>
</tr>
<tr>
<td>56</td>
<td>hsm-group-down</td>
<td>HSM operation failed.</td>
</tr>
<tr>
<td>57</td>
<td>hsm-group-up</td>
<td>HSM operation succeeded.</td>
</tr>
<tr>
<td>59</td>
<td>reporting-service-working</td>
<td>Reporting service is working.</td>
</tr>
<tr>
<td>60</td>
<td>reporting-service-failed</td>
<td>Reporting service failed.</td>
</tr>
<tr>
<td>61</td>
<td>reporting-service-inactive</td>
<td>Reporting service inactive.</td>
</tr>
<tr>
<td>62</td>
<td>dns-cache-acceleration-working</td>
<td>DNS cache acceleration is working.</td>
</tr>
<tr>
<td>63</td>
<td>dns-cache-acceleration-failed</td>
<td>DNS cache acceleration failed.</td>
</tr>
<tr>
<td>64</td>
<td>dns-cache-acceleration-inactive</td>
<td>DNS cache acceleration inactive.</td>
</tr>
<tr>
<td>65</td>
<td>ocsp-responders-ok</td>
<td>All OCSP responders are available.</td>
</tr>
<tr>
<td>66</td>
<td>ocsp-responder-failed</td>
<td>At least one OCSP responder has become unavailable.</td>
</tr>
<tr>
<td>67</td>
<td>ocsp-responders-unavailable</td>
<td>All OCSP responders are out of service.</td>
</tr>
<tr>
<td>68</td>
<td>cas-inactive</td>
<td>Certificate authentication service is inactive.</td>
</tr>
<tr>
<td>69</td>
<td>subgrid-attached</td>
<td>In a Multi-Grid configuration, sub Grid is attached to the Master Grid.</td>
</tr>
<tr>
<td>70</td>
<td>subgrid-detached</td>
<td>In a Multi-Grid configuration, sub Grid is detached from the Master Grid.</td>
</tr>
<tr>
<td>71</td>
<td>snapshot-disabled</td>
<td>In a Multi-Grid configuration, the snapshot of the Grid's current state is disabled.</td>
</tr>
<tr>
<td>72</td>
<td>snapshot-enabled</td>
<td>In a Multi-Grid configuration, the snapshot of the Grid's current state is enabled.</td>
</tr>
<tr>
<td>73</td>
<td>lb-device-up</td>
<td>Load balancer device is working.</td>
</tr>
<tr>
<td>74</td>
<td>lb-device-down</td>
<td>Load balancer device is down.</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>76</td>
<td>ldap-servers-ok</td>
<td></td>
</tr>
<tr>
<td>77</td>
<td>ldap-server-failure</td>
<td></td>
</tr>
<tr>
<td>78</td>
<td>ldap-servers-unavailable</td>
<td></td>
</tr>
<tr>
<td>79</td>
<td>ldap-service-inactive</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>sgm-state-online</td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>sgm-state-offline</td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>discovery-consolidator-service-working</td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>discovery-consolidator-service-warning</td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>discovery-consolidator-service-failed</td>
<td></td>
</tr>
<tr>
<td>85</td>
<td>discovery-consolidator-service-inactive</td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>discovery-collector-service-working</td>
<td></td>
</tr>
<tr>
<td>87</td>
<td>discovery-collector-service-warning</td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>discovery-collector-service-failed</td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>discovery-collector-service-inactive</td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>threat-protection-service-working</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>threat-protection-service-warning</td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>threat-protection-service-failed</td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>threat-protection-service-inactive</td>
<td></td>
</tr>
<tr>
<td>94</td>
<td>mgm-external-storage-disabled</td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>dns-integrity-check-failed</td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>dns-integrity-check-working</td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>dns-integrity-check-severity-indetermined</td>
<td></td>
</tr>
<tr>
<td>98</td>
<td>dns-integrity-check-severity-normal</td>
<td></td>
</tr>
<tr>
<td>99</td>
<td>dns-integrity-check-severity-informational</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>dns-integrity-check-severity-warning</td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>dns-integrity-check-severity-severe</td>
<td></td>
</tr>
<tr>
<td>102</td>
<td>dns-integrity-check-severity-critical</td>
<td></td>
</tr>
<tr>
<td>103</td>
<td>cloud-api-service-working</td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>cloud-api-service-failed</td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>cloud-api-service-inactive</td>
<td></td>
</tr>
<tr>
<td>106</td>
<td>dns-service-dtc-failed</td>
<td></td>
</tr>
<tr>
<td>107</td>
<td>raid-status-is-unavailable</td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>raid-status-is-available</td>
<td></td>
</tr>
<tr>
<td>109</td>
<td>ipmi-device-warning</td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>ipmi-device-unavailable</td>
<td></td>
</tr>
<tr>
<td>111</td>
<td>ipmi-device-available</td>
<td></td>
</tr>
<tr>
<td>112</td>
<td>rpz-refresh-working</td>
<td></td>
</tr>
</tbody>
</table>

All LDAP servers are available.
At least one LDAP server is unavailable.
All LDAP servers are unavailable.
LDAP service is inactive.
SGM is online.
SGM is offline.
Service on discovery the consolidator for Network Insight is working.
Service on discovery the consolidator for Network Insight is in warning state.
Service on discovery the consolidator for Network Insight failed.
Service on discovery the consolidator for Network Insight is inactive.
Service on discovery probes for Network Insight is working.
Service on discovery probes for Network Insight is in warning state.
Service on discovery probes for Network Insight failed.
Service on discovery probes for Network Insight is inactive.
Threat protection service for Infoblox DNS Protection is working.
Threat protection service for Infoblox DNS Protection is in warning state.
Threat protection service for Infoblox DNS Protection failed.
Threat protection service for Infoblox DNS Protection is inactive.
MGM external storage is disabled.
DNS Integrity check for authoritative zones failed.
DNS Integrity check for authoritative zones is working.
DNS Integrity check severity is None.
DNS Integrity check severity is NORMAL.
DNS Integrity check severity is INFORMATIONAL.
DNS Integrity check severity is WARNING.
DNS Integrity check severity is SEVERE.
DNS Integrity check severity is CRITICAL.
Cloud API service is working.
Cloud API service failed.
Cloud API service is inactive.
DNS sub-feature DNS Traffic Control failed.
RAID hardware status is unavailable.
RAID hardware status is available again.
IPMI device is not available.
IPMI device repeatedly is not available.
IPMI device is available again.
The `ibTrapDesc` object lists the trap messages of all Infoblox SNMP traps. This section lists all the SNMP traps by their trap types. Each trap table describes the trap message, severity, cause, and recommended actions.

**Note**: Contact Infoblox Technical Support for assistance when the recommended actions do not resolve the problems.

### Equipment Failure Traps

<table>
<thead>
<tr>
<th>OId 3.1.1.1.2.11.0</th>
<th>OId 3.1.1.1.2</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Drive Full</td>
<td></td>
<td>The primary disk drive reached 100% of usage.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Fan Monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fan &lt;n&gt; is OK</td>
<td>Informational</td>
<td>The specified fan &lt;n&gt; is functioning properly, where &lt;n&gt; indicates the fan number.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Fan &lt;n&gt; failure has occurred.</td>
<td>Minor</td>
<td>The specified fan &lt;n&gt; failed, where &lt;n&gt; indicates the fan number.</td>
<td>Inspect the specified fan for mechanical or electrical problems.</td>
</tr>
<tr>
<td>Power Supply Failure: monitored at 1 minute</td>
<td></td>
<td>The power supply failed.</td>
<td>Inspect the power supply for the possible cause of the failure.</td>
</tr>
</tbody>
</table>
### Power supply <n> failure has occurred.
**Major**
The specified power supply <n> failed, where <n> indicates the power supply number.
Inspect the specified power supply for the possible cause of the failure.

### The power supply is OK.
**Informational**
The power supply is functioning properly.
No action is required.

### Power supply <n> is OK.
**Informational**
The specified power supply <n> is functioning properly, where <n> indicates the power supply number.
No action is required.

### RAID monitoring, at 1 minute interval

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Severity</th>
<th>Description</th>
<th>Required Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>A RAID battery failure has occurred.</td>
<td>Major</td>
<td>The system RAID battery failed. The alert light is red.</td>
<td>Inspect the battery for the possible cause of the failure.</td>
</tr>
<tr>
<td>The system's RAID battery is OK.</td>
<td>Informational</td>
<td>The system RAID battery is charging and functioning properly. The alert light changed from red to green.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Unable to retrieve RAID array state!</td>
<td>Undetermined</td>
<td>The appliance failed to retrieve the RAID array state. The alert light is red.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>The system's RAID array is now running in an optimal state.</td>
<td>Informational</td>
<td>The RAID system is functioning at an optimal state.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>The system's RAID array is in a degraded state. RAID Disk &lt;n&gt; is EMPTY.</td>
<td>Major</td>
<td>The RAID system is degrading. The specified RAID Disk &lt;n&gt; is empty, where &lt;n&gt; indicates the RAID disk number.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>The system's RAID array is rebuilding. RAID Disk &lt;n&gt; is OFFLINE.</td>
<td>Minor</td>
<td>The RAID system is rebuilding. The specified RAID Disk &lt;n&gt; is offline, where &lt;n&gt; indicates the RAID disk number.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

### Syslog Backup Processes

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Severity</th>
<th>Description</th>
<th>Required Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The syslog backup process is successful.</td>
<td>Informational</td>
<td>Rotated syslog files are uploaded successfully to the external backup server.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>The syslog backup process failed.</td>
<td>Major</td>
<td>Failed to forward the rotated syslog files to the external backup server.</td>
<td>Review the syslog messages to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### Processing and Software Failure Traps

**Note:** The ibSubsystemName object is associated with certain traps of the Processing and Software Failure traps. Therefore, you cannot map all the traps of the Processing and Software Failure traps with the ibSubsystemName. If there is no value in the ibSubsystemName, then it belongs to the N/A category. For more information on the values for the ibSubsystemName, see the Table 39.7

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Severity</th>
<th>Description</th>
<th>Required Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Named Daemon Failure</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A named daemon monitoring failure has occurred.</td>
<td>Critical</td>
<td>The named process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td><strong>DHCP Daemon Failure</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A DHCP daemon monitoring failure has occurred.</td>
<td>Critical</td>
<td>The dhcpd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td><strong>SSH Daemon Failure</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>An SSH daemon failure has occurred.</td>
<td>Major</td>
<td>The sshd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>
### NTP Daemon Failure, monitored every 10 minutes

<table>
<thead>
<tr>
<th>Failure Description</th>
<th>Sev.</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An NTP daemon failure has occurred.</td>
<td>Major</td>
<td>The ntpd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### Cluster Daemon Failure

<table>
<thead>
<tr>
<th>Failure Description</th>
<th>Sev.</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A grid daemon failure has occurred.</td>
<td>Critical</td>
<td>The clusterd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### LCD Daemon Failure

<table>
<thead>
<tr>
<th>Failure Description</th>
<th>Sev.</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An LCD failure has occurred.</td>
<td>Major</td>
<td>The LCD process failed. The alert light is yellow.</td>
<td>1. Inspect the LCD panel for the possible cause of this problem. 2. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### Apache Software httpd failure, monitored every 2 minutes

<table>
<thead>
<tr>
<th>Failure Description</th>
<th>Sev.</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Apache software failure has occurred.</td>
<td>Critical</td>
<td>The request to monitor the Apache server failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### Serial Console Failure

<table>
<thead>
<tr>
<th>Failure Description</th>
<th>Sev.</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Infoblox serial console software failure has occurred.</td>
<td>Major</td>
<td>The Infoblox serial console failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### Controld Software Failure

<table>
<thead>
<tr>
<th>Failure Description</th>
<th>Sev.</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A controld failure has occurred.</td>
<td>Critical</td>
<td>The controld process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### SNMP Sub-agent Failure

<table>
<thead>
<tr>
<th>Failure Description</th>
<th>Sev.</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An SNMP server failure has occurred.</td>
<td>Major</td>
<td>The one-subagent process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### TFTP and FTPD Failure

<table>
<thead>
<tr>
<th>Failure Description</th>
<th>Sev.</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A TFTP daemon failure has occurred.</td>
<td>Critical</td>
<td>The tftpd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>An FTP daemon failure has occurred.</td>
<td>Critical</td>
<td>The ftpd process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### HTTP File Distribution, monitored at 10 second intervals

<table>
<thead>
<tr>
<th>Failure Description</th>
<th>Sev.</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An HTTP file distribution daemon failure has occurred.</td>
<td>Critical</td>
<td>The HTTP file distribution process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### DNS ONE quagga Processes (zebra & ospfd)

<table>
<thead>
<tr>
<th>Failure Description</th>
<th>Sev.</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>An OSPF routing daemon failure has occurred.</td>
<td>Critical</td>
<td>Either the zebra process or the ospf process failed. Both the zebra and ospf process belongs to ospf subsystem.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### Backup Failure

<table>
<thead>
<tr>
<th>Failure Description</th>
<th>Sev.</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Backup failed. | Minor | The backup failed. One of the following could be the cause of the failure:  
- The appliance could not access a backup directory.  
- The backup was interrupted by one of the following signals: SIGINT, SIGHUP, or SIGTERM.  
- Incorrect login or connection failure in an FTP backup.  
- The backup failed to create temporary files. | Review the syslog file to identify the possible cause of this problem. |

### Database Backup Failure

<table>
<thead>
<tr>
<th>Failure Description</th>
<th>Sev.</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database backup failed.</td>
<td>Not implemented</td>
<td>The db_dump process failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

### Backup Module Failure

<table>
<thead>
<tr>
<th>Failure Description</th>
<th>Sev.</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
</table>

### Backup File Size Exceeded
<table>
<thead>
<tr>
<th>Event</th>
<th>Level</th>
<th>Description</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>File size exceeded the quota. Backup failed</td>
<td>Not</td>
<td>The backup failed because the file size exceeded the limit of 5GB.</td>
<td>Limit the size of the backup file to less than 5GB.</td>
</tr>
<tr>
<td>Another backup is in progress. Backup will not be performed.</td>
<td>Not</td>
<td>The backup failed because of an attempt to back up or merge files while another backup or restore was in progress.</td>
<td>Wait until the backup or restore is complete before starting another backup.</td>
</tr>
<tr>
<td><strong>Watchdog Process Monitoring</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WATCHDOG: &lt;registered client name&gt; failed on &lt;server IP address&gt;</td>
<td>Critical</td>
<td>The watchdog process detected a registered client failure on a specific server. The &lt;registered client name&gt; could be one of the following: • Clusterd_timeout • DB_Sentinel • Process_Manager • Clusterd_monitor • Disk_monitor</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td><strong>Microsoft Server</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft server &lt;hostname&gt;/&lt;IP address&gt; has failed.</td>
<td>Major</td>
<td>The Microsoft server could not be reached.</td>
<td>Check that the Microsoft server is connected to the network and configured properly.</td>
</tr>
<tr>
<td>Microsoft server &lt;hostname&gt;/&lt;IP address&gt; is OK.</td>
<td>Informational</td>
<td>The Microsoft server can be reached and is functioning properly.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>Microsoft DNS/DHCP Service</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service connection to Microsoft DNS server &lt;hostname&gt;/&lt;IP address&gt; has failed.</td>
<td>Major</td>
<td>The Microsoft DNS service is not responding.</td>
<td>Check that the DNS service is configured and running on the Microsoft server.</td>
</tr>
<tr>
<td>Service connection to Microsoft DHCP server &lt;hostname&gt;/&lt;IP address&gt; has failed.</td>
<td>Major</td>
<td>The Microsoft DHCP service is not responding.</td>
<td>Check that the DHCP service is configured and running on the Microsoft server.</td>
</tr>
<tr>
<td>Service connection to Microsoft DNS server &lt;hostname&gt;/&lt;IP address&gt; is OK.</td>
<td>Informational</td>
<td>The Microsoft DNS service is responding.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Service connection to Microsoft DHCP server &lt;hostname&gt;/&lt;IP address&gt; is OK.</td>
<td>Informational</td>
<td>The Microsoft DHCP service is responding.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>NAC Authentication Server Group</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAC Authentication server group is down</td>
<td>Major</td>
<td>None of the servers in the NAC authentication server group can be reached.</td>
<td>Review the syslog.</td>
</tr>
<tr>
<td>NAC Authentication server group is up</td>
<td>Informational</td>
<td>The NAC authentication server group is responding.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>GUI Login</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A GUI login failure has occurred</td>
<td>Major</td>
<td>An admin failed to log in to the GUI.</td>
<td>Check the credentials of the admin.</td>
</tr>
<tr>
<td><strong>Serial Console Login</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A Serial Console login failure has occurred</td>
<td>Major</td>
<td>An admin failed to log in through the serial console.</td>
<td>Check the credentials and permissions, and check that the serial console is enabled.</td>
</tr>
<tr>
<td><strong>Reboot</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system is rebooting.</td>
<td>Informational</td>
<td>A system reboot command was sent.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>DHCP Lease Conflict</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP address conflicts with an existing lease.</td>
<td>Major</td>
<td>The discovery process found a DHCP lease conflict.</td>
<td>In the IP Map or List panel, select a conflicting address, and then click Resolve Conflict. For more information, see Resolving DHCP Lease Conflicts.</td>
</tr>
<tr>
<td><strong>DHCP Fixed Address Conflict</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP address conflicts with an existing fixed address.</td>
<td>Major</td>
<td>The discovery process found a fixed address conflict.</td>
<td>In the IP Map or List panel, select a conflicting address, and then click Resolve Conflict. For more information, see Resolving Fixed Address Conflicts.</td>
</tr>
<tr>
<td><strong>DHCP Range Conflict</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Type</td>
<td>Severity</td>
<td>Description</td>
<td>Action</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>DHCP address conflicts with an existing range.</td>
<td>Major</td>
<td>The discovery process found a conflict with an existing range.</td>
<td>In the IP Map or List panel, select a conflicting address, and then click Resolve Conflict. For more information, see Resolving DHCP Range Conflicts.</td>
</tr>
<tr>
<td>DHCP Host Conflict</td>
<td>Major</td>
<td>The discovery process found a conflict with an existing host address.</td>
<td>In the IP Map or List panel, select a conflicting address, and then click Resolve Conflict. For more information, see Resolving Host Conflicts.</td>
</tr>
<tr>
<td>DNS Health Check Monitor</td>
<td>Major</td>
<td>DNS Health Check query failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>DNS Health Check query has succeeded</td>
<td>Informational</td>
<td>DNS Health Check query has succeeded.</td>
<td>No action required.</td>
</tr>
<tr>
<td>Syslog Daemon Failure</td>
<td>Critical</td>
<td>Syslog daemon is not running.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>BFD Daemon Failure</td>
<td>Major</td>
<td>An BFD daemon failure has occurred.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Process Stop/Start</td>
<td>Major</td>
<td>The system stopped and started a process.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Zone Transfer Failed</td>
<td>Major</td>
<td>A zone transfer failure has occurred.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>RPZ Refresh Failed</td>
<td>Critical</td>
<td>An RPZ refresh has failed. The appliance sends this trap only when RPZ refresh from all the configured primary servers fail.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Unbound Software Failed</td>
<td>Major</td>
<td>A unbound daemon monitoring failure has occurred.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Threat Analytics Service Failed</td>
<td>Major</td>
<td>Auto download for Threat Analytics has failed.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Outbound Service Failed</td>
<td>Major</td>
<td>The Outbound service failure has occurred.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Clear</td>
<td>N/A</td>
<td>The SNMP Trap for LCD failure is cleared.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>SNMP Trap is cleared. LCD failure</td>
<td>N/A</td>
<td>The SNMP Trap for LCD failure is cleared.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>SNMP Trap is cleared. Serial Console</td>
<td>N/A</td>
<td>The SNMP Trap for Serial Console is cleared.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>SNMP Trap is cleared. ControlD failure</td>
<td>N/A</td>
<td>The SNMP Trap for ControlD failure is cleared.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>SNMP Trap is cleared. GUI Login</td>
<td>N/A</td>
<td>The SNMP Trap for GUI Login is cleared.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>SNMP Trap is cleared. Serial Console Login</td>
<td>N/A</td>
<td>The SNMP Trap for Serial Console Login is cleared.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>SNMP Trap is cleared. SSHD failure</td>
<td>N/A</td>
<td>The SNMP Trap for SSHD failure is cleared.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>SNMP Trap is cleared. LDAP servers</td>
<td>N/A</td>
<td>The SNMP Trap for LDAP server is cleared.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>
SNMP Trap is cleared. OCSP Responders  | N/A | The SNMP Trap for OCSP Responders is cleared. | No action is required.
SNMP Trap is cleared. OSPF  | N/A | The SNMP Trap for OSPF is cleared. | No action is required.
SNMP Trap is cleared. OSPF6  | N/A | The SNMP Trap for OSPF6 is cleared. | No action is required.
SNMP Trap is cleared. BGP  | N/A | The SNMP Trap for BGP is cleared. | No action is required.
SNMP Trap is cleared. HSM  | N/A | The SNMP Trap for HSM is cleared. | No action is required.
SNMP Trap is cleared. HTTP  | N/A | The SNMP Trap for HTTP is cleared. | No action is required.
SNMP Trap is cleared. Cluster  | N/A | The SNMP Trap for Cluster is cleared. | No action is required.
SNMP Trap is cleared. DuplicateIP  | N/A | The SNMP Trap for Duplicate IP is cleared. | No action is required.

Restart
The system is being restarted. | Informational | A system restart command was sent. | No action is required.

DNS Integrity Check
Cannot perform DNS Integrity Check because the appliance is unable to connect to the external DNS server. There are list of nameservers failure: <IP addresses>  | N/A | The DNS integrity check cannot be performed because the appliance is unable to connect to the external DNS server. | No action is required.

Threshold Crossing Traps

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.2.11.0</th>
<th>ibTrapSeverity</th>
<th>ibObjectName OID 3.1.1.2.3.0</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Memory Usage</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System has run out of memory.</td>
<td>Major</td>
<td>memory</td>
<td></td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
</tbody>
</table>

- The appliance ran out of memory. The appliance encountered this problem when one of the following occurred:
  - The total free memory on the appliance was less than or equal to 0%.
  - The total physical memory was less than the total free memory.
  - The percentage of free memory compared to the total physical memory was less than 5%, and the free swap percentage was less than 80%.
  - The percentage of free memory compared to the total physical memory was less than 5%, plus the numbers of both swap INs and swap OUTs were greater than or equal to 3,200.
  - The percentage of free memory compared to the total physical memory was between 5% and 10%, the free swap percentage was greater than or equal to 80%, plus the numbers of both swap INs and swap OUTs were greater than or equal to 3,200.
  - The percentage of free memory compared to the total physical memory was greater than 10%, the free swap percentage was less than 80%, plus the numbers of both swap INs and swap OUTs were greater than or equal to 3,200.

Note: Free memory = free physical RAM + free cache buffers. The high threshold for swap pages is 3,200.
<table>
<thead>
<tr>
<th>Component</th>
<th>Level</th>
<th>Type</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
</table>
| System memory usage               | Minor   | memory     | The memory usage on the appliance exceeded the configured Trigger value. For more information, see Defining Thresholds for Traps. The appliance encountered this problem when one of the following occurred:  
  - The percentage of free memory compared to the total physical memory was less than 5%, and the free swap percentage was less than 90%.  
  - The percentage of free memory compared to the total physical memory was less than 5%, plus the number of swap INs was less than 3,200 and the number of swap OUTs was greater than or equal to 3,200.  
  - The percentage of free memory compared to the total physical memory was between 5% and 10%, and the free swap percentage was less than 80%.  
  - The percentage of free memory compared to the total physical memory was greater than 5%, plus the number of swap INs was less than 3,200 and the number of swap OUTs was greater than or equal to 3,200.  
  
  **Note:** Free memory = free physical RAM + free cache buffers.  
  The high threshold for swap pages is 3,200.  
  Review the syslog file to identify the possible cause of this problem. | Review the syslog file to identify the possible cause of this problem. |
| System memory usage is OK.        | Minor   | memory     | The memory usage on the system is at or below the Reset value after it went above the Trigger value.                                                                                                      | No action is required.                                                 |
| Primary Hard Drive Usage (monitored every 30 seconds) |         |            |                                                                                                                                                                                                  |                                                                        |
| System primary hard disk usage is over threshold value. | Minor   | disk_usage | The appliance sends this trap when primary hard disk usage first exceeds the configured Trigger value. The default value is 85. The alert light is yellow. For more information, see Defining Thresholds for Traps. | Review the syslog file to identify the possible cause of this problem. |
| Primary drive is full.            | Major   | disk_usage | The primary hard disk usage exceeded 95%. The alert light is red.                                                                                                                                 | Review the syslog file to identify the possible cause of this problem. |
| Primary drive usage is OK.        | Minor   | disk_usage | The appliance sends this trap when the primary hard disk usage first moves at or below the configured Reset value after it exceeded the Trigger value. The default is 70. The alert light is green. | No action is required.                                                 |
| CPU Usage                         | Major   | cpu_usage  | CPU usage exceeded the Trigger value for 15 seconds. For more information, see Defining Thresholds for Traps.                                                                                                                                 | Monitor CPU usage.                                                    |
| CPU usage OK.                     | Minor   | cpu_usage  | CPU usage dipped below the reset value after the "CPU usage above threshold value" trap was sent.                                                                                                                                 | No action is required.                                                 |
| Note: Use the CLI command set throttletrap to enable the CPU usage trap and configure the trigger and reset values. For information, refer to the Infoblox CLI Guide. |         |            |                                                                                                                                                                                                  |                                                                        |
| Swap Usage                        | Major   | swap_usage | System swap space usage exceeded the Trigger value. For more information, see Defining Thresholds for Traps.                                                                                                                                 | Monitor System swap usage.                                            |
| Swap usage is OK.                 | Minor   | swap_usage | System swap space usage dipped below the reset value after it exceeded the Trigger value.                                                                                                                                 | No action is required.                                                 |
| Replication Statistics Monitoring | N/A     |            |                                                                                                                                                                                                  | Review the syslog file to identify the possible cause of this problem. |
| Grid queue replication problem.   | N/A     |            | The system encountered this problem when all of the following conditions occurred:  
  - The node was online.  
  - The number of the replication queue being sent from the master column was greater than 0, or the number of the queue received was greater than 0.  
  - It was more than 10 minutes since the last replication queue was sent and monitored.  
  Review the syslog file to identify the possible cause of this problem. | Review the syslog file to identify the possible cause of this problem. |
| DHCP Range Threshold Crossing     |         |            |                                                                                                                                                                                                  |                                                                        |
### DHCP High Threshold Crossed

<table>
<thead>
<tr>
<th>Member</th>
<th>Network</th>
<th>Range</th>
<th>High Trigger Mark</th>
<th>High Reset Mark</th>
<th>Current Usage</th>
<th>Active Leases</th>
<th>Available Leases</th>
<th>Total Addresses</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DHCP server node VIP&gt;</td>
<td>&lt;network&gt;/ &lt;network view&gt;</td>
<td>&lt;DHCP range&gt;/ &lt;network view&gt;</td>
<td>&lt;high percentage&gt; (95% by default)</td>
<td>&lt;reset percentage&gt; (80% by default)</td>
<td>&lt;current usage percentage&gt;</td>
<td>&lt;number of active leases&gt;</td>
<td>&lt;number of available leases&gt;</td>
<td>&lt;total addresses&gt;</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The system encountered this problem when the address usage in the DHCP range is greater than the configured High Trigger value.

Review the syslog file to identify the possible cause of this problem.

### DHCP High Threshold Reset

<table>
<thead>
<tr>
<th>Member</th>
<th>Network</th>
<th>Range</th>
<th>High Trigger Mark</th>
<th>High Reset Mark</th>
<th>Current Usage</th>
<th>Active Leases</th>
<th>Available Leases</th>
<th>Total Addresses</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DHCP server node VIP&gt;</td>
<td>&lt;network&gt;/ &lt;network view&gt;</td>
<td>&lt;DHCP range&gt;/ &lt;network view&gt;</td>
<td>&lt;high percentage&gt; (95% by default)</td>
<td>&lt;reset percentage&gt; (80% by default)</td>
<td>&lt;current usage percentage&gt;</td>
<td>&lt;number of active leases&gt;</td>
<td>&lt;number of available leases&gt;</td>
<td>&lt;total addresses&gt;</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The system encountered this problem when the address usage in the DHCP range goes below the Reset value after it hit the Trigger value.

### IPAM Utilization Threshold Crossing

<table>
<thead>
<tr>
<th>Network</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPAM Utilization capacity usage is over the threshold value.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The appliance sends this trap when the IPAM utilization for a network is above the configured Trigger value.

Review the syslog file to identify the possible cause of this problem.

<table>
<thead>
<tr>
<th>Network Container</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPAM Utilization capacity usage is over the threshold value.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The appliance sends this trap when the IPAM utilization for a network container is above the configured Trigger value.

Review the syslog file to identify the possible cause of this problem.

<table>
<thead>
<tr>
<th>Network</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPAM Utilization capacity usage is OK.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The appliance sends this trap when the IPAM utilization for a network is below the configured Reset value.

Review the syslog file to identify the possible cause of this problem.

<table>
<thead>
<tr>
<th>Network Container</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPAM Utilization capacity usage is OK.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The appliance sends this trap when the IPAM utilization for a network container is below the configured Reset value.

Review the syslog file to identify the possible cause of this problem.
<table>
<thead>
<tr>
<th>DHCP DNS Updates Deferred</th>
<th>N/A</th>
<th>Threshold</th>
<th>The DNS updates were deferred because of DDNS update errors.</th>
<th>Review the syslog file to identify the possible cause of this problem.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHZ Hit Rate</td>
<td>N/A</td>
<td>Threshold</td>
<td>The appliance sends this trap when the RHZ hit rate exceeds the configured Trigger value.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>RHZ hit rate has returned to normal value.</td>
<td>N/A</td>
<td>Threshold</td>
<td>The appliance sends this trap when the RHZ hit rate equals the configured Reset value.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Threat Protection Total Traffic</td>
<td>N/A</td>
<td>Threshold</td>
<td>The appliance sends this trap when the Threat Protection total traffic exceeds the configured Trigger value.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Threat Protection Service total traffic is above threshold.</td>
<td>N/A</td>
<td>Threshold</td>
<td>The appliance sends this trap when the Threat Protection total traffic is less than the configured Reset value.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Threat Protection Service dropped traffic is above threshold.</td>
<td>N/A</td>
<td>Threshold</td>
<td>The appliance sends this trap when the Threat Protection dropped traffic exceeds the configured Trigger value.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Threat Protection Service dropped traffic is OK.</td>
<td>N/A</td>
<td>Threshold</td>
<td>The appliance sends this trap when the Threat Protection dropped traffic is less than the configured Reset value.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Database Capacity Usage</td>
<td>Minor</td>
<td>db_usage</td>
<td>The appliance database usage exceeded the configured threshold value.</td>
<td>Increase the database capacity.</td>
</tr>
<tr>
<td>Database capacity used is OK.</td>
<td>Minor</td>
<td>db_usage</td>
<td>The appliance database usage is less than the configured threshold value.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>DNS Monitor</td>
<td>Major</td>
<td>dns_security_port</td>
<td>DNS security alert. There were actual DNS responses to invalid ports in the last minute, comprising percent% of all responses. Primary sources: ip_address sent count, ip_address sent count.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DNS security alert. There were actual DNS responses to invalid ports in the last minute, comprising percent% of all responses. Primary sources: ip_address sent count, ip_address sent count.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>where</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>actual is the total number of DNS responses arrive on invalid ports.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>percent% is the percentage of invalid DNS responses over the total number of DNS responses.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ip_address is the IP address of the primary source that generated the invalid DNS responses.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>count is the number of invalid responses generated by the specified IP address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Example: DNS security alert. There were 1072 DNS responses to invalid ports in the last minute, comprising 92% of all responses. Primary sources: 10.0.0.0 sent 1058, 2.2.2.2 sent 14.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. Review the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DNS alert status</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• syslog file</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Limit access or block connections from the primary sources. For information, see Configuring Rate Limiting Rules.</td>
<td></td>
</tr>
</tbody>
</table>
DNS security alert. There were actual DNS responses with invalid TXID in the last minute, comprising percent% of all responses. Primary sources: ip_address sent count, ip_address sent count.

where
- actual is the total number of DNS responses that have invalid TXIDs
- percent% is the percentage of invalid DNS responses over the total number of DNS responses.
- ip_address is the IP address of the primary source that generated the invalid DNS responses.
- count is the number of invalid responses generated by the specified IP address.

Example:
DNS security alert. There were 1072 DNS responses with invalid TXID in the last minute, comprising 92% of all responses. Primary sources: 10.0.0.0 sent 1058, 2.2.2.2 sent 14.

1. Review the following:
   - DNS alert status
   - syslog file
2. Limit access or block connections from the primary sources.

   For information, see Configuring Rate Limiting Rules.

### RootFS Partition Monitor

<table>
<thead>
<tr>
<th>Status</th>
<th>Severity</th>
<th>Description</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root file system is full.</td>
<td>Major</td>
<td>Root filesystem usage exceeded the maximum.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Root file system disk usage is over threshold value.</td>
<td>Minor</td>
<td>Root filesystem usage first exceeds the configured Trigger value.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Root file system disk usage is OK.</td>
<td>Minor</td>
<td>Root filesystem usage first moves at or below the configured Reset value after it exceeded the Trigger value. For information on setting the Trigger and Reset values, see Defining Thresholds for Traps.</td>
<td>No action</td>
</tr>
</tbody>
</table>

### Reporting

<table>
<thead>
<tr>
<th>Status</th>
<th>Severity</th>
<th>Description</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting drive is full.</td>
<td>Major</td>
<td>Reporting drive reached the maximum capacity.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Reporting drive usage is over threshold value.</td>
<td>Minor</td>
<td>The appliance sends this trap when the Reporting volume usage first exceeds the configured Trigger value.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>Reporting drive usage is OK.</td>
<td>Minor</td>
<td>The appliance sends this trap when the Reporting volume usage first moves at or below the configured Reset value after it exceeded the Trigger value. For information on setting the Trigger and Reset values, see Defining Thresholds for Traps.</td>
<td>No action</td>
</tr>
</tbody>
</table>

### File Distribution

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>File distribution service storage reached the configured threshold value.</td>
<td>Review the syslog file to identify the possible cause of this problem.</td>
<td></td>
</tr>
</tbody>
</table>

### Object State Change Traps

<table>
<thead>
<tr>
<th>_oid</th>
<th>ibTrapSeverity</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibTrapDesc</td>
<td>service shutdown</td>
<td>Major</td>
<td>The appliance is shutting down its services while synchronizing the database with the Grid Master.</td>
</tr>
</tbody>
</table>
| Network Interfaces Monitoring

LAN1 port link is down. Please check the connection. | Major | The LAN1 port is up, but the link is down. | Check the LAN1 link connection. |
LAN2 port link is down. Please check the connection. | Major | The LAN2 port is up, but the link is down. | Check the LAN2 link connection. |
HA port link is down. Please check the connection. | Major | The HA port is up, but the link is down. | Check the HA link connection. |
MGMT port link is down. Please check the connection. | Major | The MGMT port is enabled, but the link is down. | Check the MGMT link connection. |
LAN1 port link is up. | Major | The LAN1 port link is up and running. | No action is required. |
LAN2 port link is up. | Major | The LAN2 port link is up and running. | No action is required. |
HA port link is up. | Major | The HA port link is up and running. | No action is required. |
<table>
<thead>
<tr>
<th>Event Description</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGMT port link is up.</td>
<td>Major</td>
<td>The MGMT port link is up and running. No action is required.</td>
</tr>
<tr>
<td>HA State Change from Initial to Active</td>
<td>Informational</td>
<td>The node has become ACTIVE. A node in an HA pair becomes active. The HA pair starts up. No action is required.</td>
</tr>
<tr>
<td>HA State Change from Passive to Active</td>
<td>Informational</td>
<td>The node has become ACTIVE. The node changed from a passive to an active node. No action is required.</td>
</tr>
<tr>
<td>HA State Change to Active-Active</td>
<td>Informational</td>
<td>The node is in an ACTIVE-ACTIVE state. The node is in the active state. No action is required.</td>
</tr>
<tr>
<td>HA State Change from Initial to Passive</td>
<td>Informational</td>
<td>The node has become PASSIVE. A node in an HA pair becomes passive. The HA pair starts up, and the node is not a Grid Master candidate. No action is required.</td>
</tr>
<tr>
<td>Node Connected to Grid</td>
<td>Informational</td>
<td>The Grid member is connected to the Grid master. The Grid member joined the Grid, and it is not a Grid Master candidate. No action is required.</td>
</tr>
<tr>
<td>Node Disconnected from Grid</td>
<td>Informational</td>
<td>The Grid member is not connected to the Grid master. The Grid member lost its connection to the Grid Master. No action is required.</td>
</tr>
<tr>
<td>Replication State Monitoring</td>
<td>Informational</td>
<td>HA replication is online. The HA replication is online. No action is required.</td>
</tr>
<tr>
<td></td>
<td>Informational</td>
<td>HA replication is offline. The HA replication is offline. No action is required.</td>
</tr>
<tr>
<td>NTP is out of sync, monitored every 30 seconds</td>
<td>Major</td>
<td>The NTP service is out of synchronization. The Infoblox NTP server and the external NTP server are not synchronized. Review the syslog file to identify the possible cause of this problem.</td>
</tr>
<tr>
<td>NTP Service is working.</td>
<td>Informational</td>
<td>The NTP service started working again. No action is required.</td>
</tr>
<tr>
<td>NTP service is synchronizing to local clock</td>
<td>Major</td>
<td>The NTP service resumed synchronization. The Infoblox NTP server synchronizes its clients with its local clock. No action is required.</td>
</tr>
<tr>
<td>DHCP service state change</td>
<td>Informational</td>
<td>DHCP Service is working. The DHCP service started working again. No action is required.</td>
</tr>
<tr>
<td></td>
<td>Informational</td>
<td>DHCP Service is in a warning state. The DHCP service is in a warning state. Review the syslog file.</td>
</tr>
<tr>
<td></td>
<td>Informational</td>
<td>DHCP Service is inactive. The DHCP service became inactive. Check if an admin disabled the service.</td>
</tr>
<tr>
<td>DNS service state change</td>
<td>Informational</td>
<td>DNS Service is working. The DNS service started working again. No action is required.</td>
</tr>
<tr>
<td></td>
<td>Informational</td>
<td>DNS Service is in a warning state. The DNS service is in a warning state. Review the syslog file.</td>
</tr>
<tr>
<td></td>
<td>Informational</td>
<td>DNS Service is inactive. The DNS service became inactive. Check if an admin disabled the service.</td>
</tr>
<tr>
<td>NTP service state change</td>
<td>Informational</td>
<td>The NTP service resumed synchronization. The NTP service started working again. No action is required.</td>
</tr>
<tr>
<td></td>
<td>Informational</td>
<td>NTP Service is inactive. The NTP service became inactive. Check if an admin disabled the service.</td>
</tr>
<tr>
<td>TFTP service state change</td>
<td>Informational</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>State</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TFTP Service</td>
<td>Working</td>
<td>The TFTP service started working again.</td>
</tr>
<tr>
<td>TFTP Service</td>
<td>Inactive</td>
<td>The TFTP service became inactive.</td>
</tr>
<tr>
<td>FTP service state change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP Service</td>
<td>Working</td>
<td>The FTP service started working again.</td>
</tr>
<tr>
<td>FTP Service</td>
<td>Inactive</td>
<td>The FTP service became inactive.</td>
</tr>
<tr>
<td>HTTP service state change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP File Dist Service</td>
<td>Working</td>
<td>The HTTP file distribution service started working again.</td>
</tr>
<tr>
<td>HTTP File Dist Service</td>
<td>Inactive</td>
<td>The HTTP file distribution service became inactive.</td>
</tr>
<tr>
<td>bloxTools service state change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BloxTools Service</td>
<td>Working</td>
<td>The bloxTools service started working again.</td>
</tr>
<tr>
<td>BloxTools Service</td>
<td>Inactive</td>
<td>The bloxTools service became inactive.</td>
</tr>
<tr>
<td>BloxTools Service</td>
<td>In warning state</td>
<td>The bloxTools service is in a warning state.</td>
</tr>
<tr>
<td>Captive Portal service state change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Captive Portal Service</td>
<td>Working</td>
<td>The captive portal service started working again.</td>
</tr>
<tr>
<td>Captive Portal Service</td>
<td>Inactive</td>
<td>The captive portal service became inactive.</td>
</tr>
<tr>
<td>Discovery Collector service state change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery Collector Service</td>
<td>Working</td>
<td>The discovery collector service started working again.</td>
</tr>
<tr>
<td>Discovery Collector Service</td>
<td>Inactive</td>
<td>The discovery collector service became inactive.</td>
</tr>
<tr>
<td>Discovery Collector Service</td>
<td>In warning state</td>
<td>The discovery collector service is in a warning state.</td>
</tr>
<tr>
<td>Discovery Collector Service</td>
<td>Failed</td>
<td>The discovery collector service has failed.</td>
</tr>
<tr>
<td>Discovery Collector service state change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery Consolidator Service</td>
<td>Working</td>
<td>The discovery consolidator service started working again.</td>
</tr>
<tr>
<td>Discovery Consolidator Service</td>
<td>Inactive</td>
<td>The discovery consolidator service became inactive.</td>
</tr>
<tr>
<td>Discovery Consolidator Service</td>
<td>In warning state</td>
<td>The discovery consolidator service is in a warning state.</td>
</tr>
<tr>
<td>Discovery Consolidator Service</td>
<td>Failed</td>
<td>The discovery consolidator service has failed.</td>
</tr>
<tr>
<td>IF-MAP service state change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IFMAP Service</td>
<td>Inactive</td>
<td>The IF-MAP service became inactive.</td>
</tr>
<tr>
<td>IFMAP Service</td>
<td>Working</td>
<td>The IF-MAP service started working again.</td>
</tr>
<tr>
<td>LDAP service state change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP Service</td>
<td>Inactive</td>
<td>The LDAP service became inactive.</td>
</tr>
</tbody>
</table>

Copyright ©2019, Infoblox, Inc. All right reserved.
<table>
<thead>
<tr>
<th>Event Description</th>
<th>Status</th>
<th>Detailed Description</th>
<th>Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>All LDAP servers are available.</td>
<td>Informational</td>
<td>All LDAP servers are available.</td>
<td>No action is required.</td>
</tr>
</tbody>
</table>
| At least one LDAP server is unavailable.                                         | Major      | At least one LDAP server is out of service.                                           | • Check if an admin disabled the LDAP server.  
• Review the syslog file.                                                          |
| All LDAP servers are unavailable.                                                | Informational | All LDAP servers are not available.                                                    | • Check if an admin disabled the LDAP server.  
• Review the syslog file.                                                          |
| Certificate Authentication Service state change                                   |            |                                                                                        |                                             |
| CAS service is working.                                                           | Informational | The certificate authentication service started working again.                        | No action is required.                      |
| CAS service is inactive.                                                          | Informational | The certificate authentication service became inactive.                                | Check if an admin disabled the service.      |
| OCSP responders state change                                                      |            |                                                                                        |                                             |
| All OCSP responders available.                                                    | Informational | The OCSP responders are available.                                                     | No action is required.                      |
| All OCSP responders are out of service.                                           | Informational | The OCSP responders are out of service.                                                | • Check if an admin disabled the service.      
• Review the syslog file.                                                          |
| OCSP service inactive.                                                            | Informational | The OCSP responders service became inactive.                                           | • Check if an admin disabled the service.      
• Review the syslog file.                                                          |
| Reporting service state change                                                    |            |                                                                                        |                                             |
| Reporting Service is working.                                                     | Informational | The Reporting service started working again.                                          | No action is required.                      |
| Reporting Service is inactive.                                                    | Informational | The Reporting service became inactive.                                                | Check if an admin disabled the service.      |
| Reporting Service is in warning state.                                            | Informational | The Reporting service is in warning state.                                            | Review the audit log file.                  |
| Threat Analytics state change                                                     |            |                                                                                        |                                             |
| Threat Analytics Service is working.                                              | Informational | The Threat Analytics service started working again.                                   | No action is required.                      |
| Threat Analytics Service is inactive.                                             | Informational | The Threat Analytics service became inactive.                                         | Check if an admin disabled the service.      |
| Threat Analytics Service is failed.                                               | Informational | The Threat Analytics service has failed.                                              | Review the audit log file.                  |
| Threat Analytics Service is in warning state.                                     | Informational | The Threat Analytics service is in warning state.                                     | Review the audit log file.                  |
| RPZ refresh state change                                                          |            |                                                                                        |                                             |
| RPZ refresh is OK.                                                                | Informational | An RPZ refresh succeeded. The appliance sends this trap every time an RPZ zone transfer is successful. | No action is required.                      |
| Cisco ISE service state change                                                    |            |                                                                                        |                                             |
| Cisco ISE server is OK.                                                           | Informational | The Cisco ISE service started working again.                                          | No action is required.                      |
| Connection Error has occurred in Cisco ISE server.                                | Informational | There is a loss of connection between the NIOS appliance and Cisco ISE server.        | • Check if an admin disabled the service.      
• Review the audit log file.                                                        |
| Cloud API service state change                                                    |            |                                                                                        |                                             |
### Cloud API service state change

<table>
<thead>
<tr>
<th>Status</th>
<th>Level</th>
<th>Description</th>
<th>Action(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud API service is working.</td>
<td>Informational</td>
<td>The Cloud API service started working again.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Cloud API service is inactive.</td>
<td>Informational</td>
<td>The Cloud API service became inactive</td>
<td>• Check if an admin disabled the Cloud API service.</td>
</tr>
<tr>
<td>Cloud API service has failed.</td>
<td>Critical</td>
<td>The Cloud API service has failed.</td>
<td>• Review the audit log file.</td>
</tr>
</tbody>
</table>

### DNS Integrity Check state change

<table>
<thead>
<tr>
<th>Status</th>
<th>Level</th>
<th>Description</th>
<th>Action(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Integrity Check is working.</td>
<td>Informational</td>
<td>The DNS Integrity Check started working again.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>DNS Integrity Check failed.</td>
<td>Informational</td>
<td>The DNS Integrity Check has failed.</td>
<td>• Check if an admin disabled the service.</td>
</tr>
<tr>
<td>DNS Integrity Check severity has changed.</td>
<td>Informational</td>
<td>The DNS Integrity Check has changed.</td>
<td>Review the syslog file.</td>
</tr>
</tbody>
</table>

### TAXII service state change

<table>
<thead>
<tr>
<th>Status</th>
<th>Level</th>
<th>Description</th>
<th>Action(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAXII service is working.</td>
<td>Informational</td>
<td>The TAXII service started working again.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>TAXII Service is failed.</td>
<td>Informational</td>
<td>The TAXII service has failed.</td>
<td>• Check if an admin disabled the service.</td>
</tr>
<tr>
<td>TAXII service is inactive.</td>
<td>Informational</td>
<td>The TAXII service became inactive.</td>
<td>• Review the audit log file.</td>
</tr>
<tr>
<td>TAXII Service is in warning state.</td>
<td>Informational</td>
<td>The TAXII service is in warning state.</td>
<td>Review the audit log file.</td>
</tr>
</tbody>
</table>

### Outbound service state change

<table>
<thead>
<tr>
<th>Status</th>
<th>Level</th>
<th>Description</th>
<th>Action(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Outbound Service Manager stopped.</td>
<td>Informational</td>
<td>The Outbound service manager has stopped working.</td>
<td>• Check if an admin disabled the service.</td>
</tr>
<tr>
<td>The Outbound Service Manager failed.</td>
<td>Major</td>
<td>The Outbound service manager has failed.</td>
<td>• Review the audit log file.</td>
</tr>
<tr>
<td>The Outbound Service Manager started.</td>
<td>Informational</td>
<td>The Outbound service manager has started.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>The Outbound worker failed.</td>
<td>Major</td>
<td>The Outbound worker has failed.</td>
<td>Review the audit log file.</td>
</tr>
</tbody>
</table>

### IPMI Device state change

<table>
<thead>
<tr>
<th>Status</th>
<th>Level</th>
<th>Description</th>
<th>Action(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPMI is used by some hardware monitors to test hardware health. The IPMI Device has not responded. Hardware monitors may show spurious failures.</td>
<td>Informational</td>
<td>The IPMI Device has not responded.</td>
<td>• Check if an admin disabled the IPMI interface.</td>
</tr>
<tr>
<td>IPMI Device failed.</td>
<td>Major</td>
<td>The IPMI Device has failed.</td>
<td>• Review the audit log file.</td>
</tr>
</tbody>
</table>
IPMI is used by some hardware monitors to test hardware health. Because the IPMI Device has not responded for a while, hardware monitor failures are likely to be spurious.

Informational  The IPMI Device has not responded.

- Check if an admin disabled the IPMI interface.
- Review the audit log file.

IPMI is used by some hardware monitors to test hardware health. The IPMI Device is now available; subsequent hardware monitor failures are likely to be genuine.

Informational  The IPMI Device is now available  No action required.

**Process Started and Stopped Traps**

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibTrapSeverity</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Httpd Start</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The process started normally.</td>
<td>Informational</td>
<td>The httpd process started.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>Httpd Stop</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The process stopped normally.</td>
<td>Informational</td>
<td>The httpd process stopped.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>Process Stop/Start</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system stopped and started a process.</td>
<td>Major</td>
<td>The system restarted a process.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>Zone Transfer Failed</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A zone transfer failure has occurred.</td>
<td>Critical</td>
<td>A zone transfer failed.</td>
<td>Review the syslog file</td>
</tr>
</tbody>
</table>

**Revoked License Trap**

<table>
<thead>
<tr>
<th>ibTrapDesc OID 3.1.1.1.2.11.0</th>
<th>ibTrapSeverity</th>
<th>Description/Cause</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revoked License</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>This trap is generated when a license is revoked</td>
<td>Critical</td>
<td>A license was revoked.</td>
<td>Obtain and install new license</td>
</tr>
</tbody>
</table>

**ibPlatformOne MIB**

The `ibPlatformOne MIB` provides information about the CPU temperature of the appliance, the replication status, the average latency of DNS requests, DNS security alerts, CPU and memory utilization of the appliance, and the Infoblox service status. Figure 39.4 illustrates the structure of the PlatformOne MIB. (Note that the OIDs in the illustration do not include the prefix .1.3.6.1.4.1.7779.)

The `ibPlatformOne MIB` contains the following objects:

- `ibCPUTemperature` (IbString) tracks the CPU temperature of the appliance.
- `ibClusterReplicationStatusTable` provides information in tabular format about the replication status of the appliance. For information, see `ibClusterReplicationStatusTable`.
- `ibNetworkMonitor` provides information about the average latency of authoritative and nonauthoritative replies to DNS queries for different time intervals. It also provides information about invalid DNS responses that arrive on invalid ports or have invalid DNS transaction IDs. For information, see `ibNetworkMonitor`.
- `ibHardwareType` (IbString) provides information about the hardware platform. For an Infoblox appliance, it provides the model number of the Infoblox hardware platform. For vNIOS appliances, it identifies whether the hardware platform is Riverbed or VMware.
- `ibHardwareId` (IbString) provides the hardware ID of the NIOS appliance.
- `ibSerialNumber` (IbString) provides the serial number of the Infoblox hardware platform.
- `ibNiosVersion` (IbString) provides the version of the NIOS software.
- `ibSystemMonitor` provides information about the CPU and memory utilization of the appliance. For information, see `ibSystemMonitor`.
- `ibGridStatus` provides information about an appliance. It indicates whether the appliance is a Grid Master, member, or an independent appliance.
- `ibHAStatus` provides information about the HA status of a member. It indicates if the member is part of an HA configuration, and if it is the active or passive node.
- `ibGridMasterCandStatus` indicates if a member is a Grid Master candidate.
- `ibGridMasterVIP` provides the Grid Master virtual IP address.
- `ibGridReplicationState` provides information about the replication status.

The `ibPlatformOne MIB` also contains the following tables that provide status of the Infoblox services as well as system and hardware services on the appliance you query:
• ibMemberServiceStatusTable provides status of the Infoblox services, such as the DNS and DHCP services, on a queried appliance. For information, see `ibMemberServiceStatusTable`.

• ibMemberNodeServiceStatusTable provides status of the system and hardware services on a queried appliance. For information, see `ibMemberNodeServiceStatusTable`.

• ibMemberPassiveNodeServiceStatusTable provides status of the system and hardware services on the passive node of an HA pair if the queried appliance is the VIP or the active node of an HA pair. For independent appliances and the passive nodes of HA pairs, this table does not display any status. For information, see `ibMemberPassiveNodeServiceStatusTable`.

Figure 39.4 ibPlatformOne MIB Structure
ibClusterReplicationStatusTable

ibClusterReplicationStatusTable (object ID 3.1.1.2.1.2.1.1) provides information about the Grid replication status. For information about Infoblox
SNMP traps, see ibTrapDesc (OID 3.1.1.1.2.11.0).

Figure 39.5 shows the sub branches of ibClusterReplicationStatusTable.

Figure 39.5 ibClusterReplicationStatusTable Objects

Table 39.9 provides information about the ibClusterReplicationStatusTable objects.

Table 39.9 ibClusterReplicationStatusTable Objects

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibClusterReplicationStatusEntry</td>
<td>A conceptual row that provides information about the Grid replication status. The status indicates whether the appliance is sending replication queues, receiving queues, or having problems with the replication.</td>
</tr>
<tr>
<td>ibNodeIPAddress (IbIpAddr)</td>
<td>IP address of a Grid member.</td>
</tr>
<tr>
<td>ibNodeReplicationStatus (IbString)</td>
<td>Replication status of the Grid member. The replication status can be one of the following: online, offline, or snapshotting.</td>
</tr>
<tr>
<td>ibNodeQueueFromMaster (Integer)</td>
<td>“Sent” queue size from master.</td>
</tr>
<tr>
<td>ibNodeLastRepTimeFromMaster (IbString)</td>
<td>Last sent time from master.</td>
</tr>
<tr>
<td>ibNodeQueueToMaster (Integer)</td>
<td>“Receive” queue size from master.</td>
</tr>
<tr>
<td>ibNodeLastRepTimeToMaster (IbString)</td>
<td>Last receive time from master.</td>
</tr>
</tbody>
</table>

ibNetwork Monitor

As shown in Figure 39.6, the ibNetwork Monitor has one subtree, ibNetworkMonitorDNS, that branches out into the following:

- ibNetworkMonitorDNSActive (Integer) reports on whether DNS latency monitoring is enabled. You can enable DNS latency monitoring using the CLI command set monitor dns. For more information, see Enabling and Disabling DNS Alert Monitoring. This is the only object in this branch. When you send a query for this object, the appliance responds with either “active” (1) or “nonactive” (0).
- ibNetworkMonitorDNSNonAA provides information about the average latency of nonauthoritative replies to DNS queries for 1-, 5-, 15-, and 60-minute intervals. For information, see ibNetworkMonitorDNSNonAA Objects.
- ibNetworkMonitorDNSAA provides information about the average latency of authoritative replies to DNS queries for 1-, 5-, 15-, and 60-minute intervals. For information, see ibNetworkMonitorDNSAA Objects.
ibNetworkMonitorDNSSecurity provides information about the invalid DNS responses that arrive on invalid ports or have invalid DNS transaction IDs. ibNetworkMonitorDNSSecurity branches out into the following:

- ibNetworkMonitorDNSSecurityInvalidPort
- ibNetworkMonitorDNSSecurityInvalidTxid
- ibNetworkMonitorDNSSecurityInvalidPortOnly (Counter)
- ibNetworkMonitorDNSSecurityInvalidPortCount (Counter)
- ibNetworkMonitorDNSSecurityInvalidTxidOnly (Counter)
- ibNetworkMonitorDNSSecurityInvalidTxidCount (Counter)
- ibNetworkMonitorDNSSecurityInvalidTxidAndPort (Counter)

For information, see Table 39.12.

Figure 39.6 ibNetworkMonitorObjects

Figure 39.7 ibNetworkMonitorDNSNonAAandibNetworkMonitorDNSAASubtrees
Table 39.10 describes the objects in `ibNetworkMonitorDNSNonAA`. You can send queries to retrieve values for these objects.

**Table 39.10 ibNetworkMonitorDNSNonAA Objects**

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT1</code></td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT1AvgLatency (Integer)</code></td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT1Count (Integer)</code></td>
<td>Indicates the number of queries used to calculate the average latency of nonauthoritative replies in the last minute.</td>
</tr>
<tr>
<td><code>ibNetworkMonitorDNSNonAAT5</code></td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last five minutes.</td>
</tr>
<tr>
<td>Object (Type)</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT5AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT5Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of nonauthoritative replies in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT15</td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT15AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT15Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of nonauthoritative replies in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT60</td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT60AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT60Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of nonauthoritative replies in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT1440</td>
<td>File that contains the objects for monitoring the average latency of nonauthoritative replies to queries in the last 24 hours.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT1440AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of nonauthoritative replies to queries in the last 24 hours.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSNonAAT1440Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of nonauthoritative replies in the last 24 hours.</td>
</tr>
</tbody>
</table>

Table 39.11 describes the objects in ibNetworkMonitorDNSAA. You can send queries to retrieve values for these objects.

Table 39.11 ibNetworkMonitorDNSAA Objects

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibNetworkMonitorDNSAAT1</td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT1AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT1Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT5</td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT5AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT5Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT15</td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT15AvgLatency (Integer)</td>
<td>Indicates the average latency in microseconds of authoritative replies to queries in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT15Count (Integer)</td>
<td>Indicates the number of queries used to calculate the average latency of authoritative replies in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSAAT60</td>
<td>File that contains the objects for monitoring the average latency of authoritative replies to queries in the last 60 minutes.</td>
</tr>
<tr>
<td>Object (Type)</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidPort</td>
<td>Tracks the number of invalid DNS responses that arrive on invalid ports. For information about invalid ports, see Monitoring DNS Transactions. This object contains a subtree with six objects that track invalid ports within a certain time interval. For information, see Table 39.13.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxid</td>
<td>Tracks the number of invalid TXIDs (DNS transaction IDs). For information about invalid TXIDs, see Monitoring DNS Transactions. This object contains a subtree with six objects that track invalid TXIDs within a certain time interval. For information, see Table 39.14.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidPortOnly</td>
<td>Tracks the number of DNS responses with both of the following conditions:</td>
</tr>
<tr>
<td>(Counter)</td>
<td>• Arrive on invalid ports</td>
</tr>
<tr>
<td></td>
<td>• Have valid TXIDs</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxidOnly</td>
<td>Tracks the number of DNS responses with both of the following conditions:</td>
</tr>
<tr>
<td>(Counter)</td>
<td>• Arrive on valid ports</td>
</tr>
<tr>
<td></td>
<td>• Have Invalid TXIDs</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidPortCount</td>
<td>Tracks the total number of invalid DNS responses that arrive on invalid ports.</td>
</tr>
<tr>
<td>(Counter)</td>
<td></td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxidCount</td>
<td>Tracks the total number of DNS responses that have invalid DNS transaction IDs.</td>
</tr>
<tr>
<td>(Counter)</td>
<td></td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxidAndPort</td>
<td>Tracks the number of DNS responses with both of the following conditions:</td>
</tr>
<tr>
<td>(Counter)</td>
<td>• Arrive on invalid ports</td>
</tr>
<tr>
<td></td>
<td>• Have invalid TXIDs</td>
</tr>
</tbody>
</table>

Table 39.13 describes the objects in ibNetworkMonitorDNSSecurityInvalidPort. Table 39.13 ibNetworkMonitorDNSSecurityInvalidPort Objects

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidPort1 (Integer)</td>
<td>Tracks the number of invalid DNS responses that arrive on invalid ports in the last one minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidPort5 (Integer)</td>
<td>Tracks the number of invalid DNS responses that arrive on invalid ports in the last five minutes.</td>
</tr>
<tr>
<td>Object (Type)</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidPort15 (Integer)</td>
<td>Tracks the number of invalid DNS responses that arrive on invalid ports in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidPort60 (Integer)</td>
<td>Tracks the number of invalid DNS responses that arrive on invalid ports in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidPort1440 (Integer)</td>
<td>Tracks the number of invalid DNS responses that arrive on invalid ports in the last 24 hours.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidPortCount (Counter)</td>
<td>Tracks the total number of invalid DNS responses that arrive on invalid ports.</td>
</tr>
</tbody>
</table>

**Table 39.14** describes the objects in ibNetworkMonitorDNSSecurityInvalidTxid.

**Table 39.14 ibNetworkMonitorDNSSecurityInvalidTxid Objects**

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxid1 (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last one minute.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxid5 (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last five minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxid15 (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last 15 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxid60 (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last 60 minutes.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxid1440 (Integer)</td>
<td>Tracks the number of DNS responses that have invalid DNS transaction IDs in the last 24 hours.</td>
</tr>
<tr>
<td>ibNetworkMonitorDNSSecurityInvalidTxidCount (Counter)</td>
<td>Tracks the total number of DNS responses that have invalid DNS transaction IDs.</td>
</tr>
</tbody>
</table>

**ibSystemMonitor**

As shown in **Figure 39.4**, ibSystemMonitor (object ID 3.1.1.2.1.2.8) has the following subtrees:

- **ibSystemMonitorCpu**: Contains ibSystemMonitorCpuUsage (Integer) that reports the CPU usage of the appliance.
- **ibSystemMonitorMem**: Contains ibSystemMonitorMemUsage (Integer) that reports the memory usage of the appliance.

**Figure 39.8 ibSystemMonitor Objects**
ibMemberServiceStatusTable

As shown in Figure 39.9, ibMemberServiceStatusTable (object ID 3.1.1.2.1.2.9) has one subtree, ibMemberServiceStatusEntry, which contains the following objects:

- `ibServiceName` (String) reports the names of the Infoblox services. For a list of Infoblox services, see Infoblox Services for ibMemberServiceStatusTable.
- `ibServiceStatus` (Integer) reports the status of the Infoblox services. For a list of service status, see Service Status.
- `ibServiceDesc` (String) describes the details of the status.

ibMemberServiceStatusTable displays the current status of the Infoblox services on the appliance that you query. For an HA pair, this table displays the service status of the active node. If the appliance you query is the passive node of an HA pair, this table reflects the service status of the passive node, which can be "inactive" or "unknown."

You can also query ibMemberNodeServiceStatusTable and ibMemberPassiveNodeServiceStatusTable that display system and hardware status on the queried appliance. For information, see ibMemberNodeServiceStatusTable and ibMemberPassiveNodeServiceStatusTable.

Figure 39.9 ibMemberServiceStatusTable Objects

Infoblox Services for ibMemberServiceStatusTable

Table 39.15 lists the values and descriptions of the Infoblox services that appear in ibMemberServiceStatusTable.

Table 39.15 ibServiceName Values for ibMemberServiceStatusTable
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>dhcp</td>
<td>DHCP service</td>
</tr>
<tr>
<td>2</td>
<td>dns</td>
<td>DNS service</td>
</tr>
<tr>
<td>3</td>
<td>ntp</td>
<td>NTP service</td>
</tr>
<tr>
<td>4</td>
<td>tftp</td>
<td>File distribution using the TFTP service</td>
</tr>
<tr>
<td>5</td>
<td>http-file-dist</td>
<td>File distribution using the HTTP service</td>
</tr>
<tr>
<td>6</td>
<td>ftp</td>
<td>File distribution using the FTP service</td>
</tr>
<tr>
<td>7</td>
<td>bloxtools-move</td>
<td>Moving the bloxTools service</td>
</tr>
<tr>
<td>8</td>
<td>bloxtools</td>
<td>The bloxTools environment</td>
</tr>
<tr>
<td>9</td>
<td>node-status</td>
<td>Member status</td>
</tr>
<tr>
<td>10</td>
<td>disk-usage</td>
<td>Disk usage</td>
</tr>
<tr>
<td>11</td>
<td>enet-lan</td>
<td>LAN port</td>
</tr>
<tr>
<td>12</td>
<td>enet-lan2</td>
<td>LAN2 port</td>
</tr>
<tr>
<td>13</td>
<td>enet-ha</td>
<td>HA port</td>
</tr>
<tr>
<td>14</td>
<td>enet-mgmt</td>
<td>MGMT port</td>
</tr>
<tr>
<td>15</td>
<td>lcd</td>
<td>LCD</td>
</tr>
<tr>
<td>16</td>
<td>memory</td>
<td>Memory</td>
</tr>
<tr>
<td>17</td>
<td>replication</td>
<td>Replication service</td>
</tr>
<tr>
<td>18</td>
<td>db-object</td>
<td>Database object</td>
</tr>
<tr>
<td>19</td>
<td>raid-summary</td>
<td>RAID array</td>
</tr>
<tr>
<td>20</td>
<td>raid-disk1</td>
<td>RAID Disk 1 (For appliances with RAID arrays)</td>
</tr>
<tr>
<td>21</td>
<td>raid-disk2</td>
<td>RAID Disk 2 (For appliances with RAID arrays)</td>
</tr>
<tr>
<td>22</td>
<td>raid-disk3</td>
<td>RAID Disk 3 (For appliances with RAID arrays)</td>
</tr>
<tr>
<td>23</td>
<td>raid-disk4</td>
<td>RAID Disk 4 (For appliances with RAID arrays)</td>
</tr>
<tr>
<td>24</td>
<td>raid-disk5</td>
<td>RAID Disk 5 (For appliances with RAID arrays)</td>
</tr>
<tr>
<td>25</td>
<td>raid-disk6</td>
<td>RAID Disk 6 (For appliances with RAID arrays)</td>
</tr>
<tr>
<td>26</td>
<td>raid-disk7</td>
<td>RAID Disk 7 (For appliances with RAID arrays)</td>
</tr>
<tr>
<td>27</td>
<td>raid-disk8</td>
<td>RAID Disk 8 (For appliances with RAID arrays)</td>
</tr>
<tr>
<td>28</td>
<td>fan1</td>
<td>Fan 1</td>
</tr>
<tr>
<td>29</td>
<td>fan2</td>
<td>Fan 2</td>
</tr>
<tr>
<td>30</td>
<td>fan3</td>
<td>Fan 3</td>
</tr>
<tr>
<td>31</td>
<td>fan4</td>
<td>Fan 4</td>
</tr>
<tr>
<td>32</td>
<td>fan5</td>
<td>Fan 5</td>
</tr>
<tr>
<td>33</td>
<td>fan6</td>
<td>Fan 6</td>
</tr>
<tr>
<td>34</td>
<td>fan7</td>
<td>Fan 7</td>
</tr>
<tr>
<td>35</td>
<td>fan8</td>
<td>Fan 8</td>
</tr>
<tr>
<td>36</td>
<td>power-supply1</td>
<td>Power supply 1</td>
</tr>
</tbody>
</table>
Service Status

When you query the service status on an appliance, the response includes the status of the services. Table 39.16 shows the values and descriptions of the status. Note that for internal Grid operations, the NTP service is always in the “working” state even if it has been disabled through the Infoblox GUI.

Table 39.16 ibServiceStates Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>working</td>
<td>The service is functioning properly.</td>
</tr>
<tr>
<td>2</td>
<td>warning</td>
<td>The service is having some issues. Check the service or hardware function and the syslog to identify the problem.</td>
</tr>
<tr>
<td>3</td>
<td>failed</td>
<td>The service failed. Review the syslog to identify the problem.</td>
</tr>
<tr>
<td>4</td>
<td>inactive</td>
<td>The service is disabled or out of service.</td>
</tr>
<tr>
<td>5</td>
<td>unknown</td>
<td>The appliance cannot detect the current status of the service.</td>
</tr>
</tbody>
</table>

ibMemberNodeServiceStatusTable

As shown in Figure 39.10, ibMemberNodeServiceStatusTable (object ID 3.1.1.2.1.10) has one subtree, ibMemberNodeServiceStatusEntry, which contains the following objects:

- `ibMemberNodeServiceName` (String) reports the names of the system and hardware services. For a list of service names, see Infoblox Services for ibMemberServiceStatusTable.
- `ibMemberNodeServiceStatus` (Integer) reports the status of the services. For a list of service status, see Service Status.
- `ibMemberNodeServiceDesc` (String) describes the details of the status.

ibMemberNodeServiceStatusTable displays the current status of the system and hardware services on the appliance that you query. For example, when you query an independent appliance, this table shows the information about the independent appliance. When you query the VIP of an HA pair, this table shows the information about the active node. For the active node of the HA pair, you can also query `ibMemberPassiveNodeServiceStatusTable` to get the status of the passive node. For information, see ibMemberPassiveNodeServiceStatusTable.

Note: For an independent appliance and the passive node of an HA pair, no information is returned when you query `ibMemberPassiveNodeServiceStatusTable`. 
Figure 39.10 ibMemberNodeServiceStatusTable Objects

As shown in Figure 39.10, ibMemberNodeServiceStatusTable (object ID 3.1.1.2.1.10.1) has one subtree, ibMemberNodeServiceStatusEntry, which contains the following objects:

- ibMemberNodeServiceName (String) reports the names of the system and hardware services. For a list of service names, see Infoblox Services for ibMemberServiceStatusTable.
- ibMemberNodeServiceStatus (Integer) reports the status of the services. For a list of possible service status, see Service Status.
- ibMemberNodeServiceDesc (String) describes details of the status.

ibMemberPassiveNodeServiceStatusTable displays the current status of the system and hardware services on the passive node of an HA pair when you query the VIP of the HA pair. For independent appliances and the passive nodes of HA pairs, this table does not display any status. Figure 39.11 ibMemberPassiveNodeServiceStatusTable Objects

ibDHCPOne MIB

The ibDHCPOne MIB provides information about address usage within a subnet, DHCP lease statistics, and DHCP packet counts. It includes two
modules, ibDHCPModule for IPv4 data and ibDHCPv6Module for IPv6 data.

**ibDHCPModule**

*Figure 39.12* illustrates the structure of the ibDHCPModule. (Note that the OIDs shown in the illustration do not include the prefix .1.3.6.1.4.1.7779.) *ibDHCPModule* contains the following objects:

- **ibDHCPSubnetTable** provides statistical data about the DHCP operations of the appliance. For information, see *ibDHCPSubnetTable*.
- **ibDHCPStatistics** maintains counters for different types of packets. For information, see *ibDHCPStatistics*.
- **ibDHCPDeferredQueuesize** tracks the total number of deferred DDNS updates that are currently in the queue to be retried. When DDNS updates are deferred due to timeout or server issues, the DHCP server puts these updates in this queue.
- **ibDHCPDDNSStats** monitors the average latency for the DDNS updates in microseconds and the number of timeouts during different time intervals. For information, see *ibDHCPDDNSStats*.

*Figure 39.12 ibDHCPModule*

**ibDHCPSubnetTable**

*ibDHCPSubnetTable* provides statistical data about the DHCP operations of the appliance. It contains the following objects:

*Table 39.17 ibDHCPSubnetTable*

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDHCPSubnet Entry</td>
<td>File that contains the objects for monitoring DHCP operations on the appliance.</td>
</tr>
</tbody>
</table>
ibDHCPSubnetNetworkAddress (IbIpAddr)
The subnetworks, in IP address format, that have IP addresses for lease. A subnetwork may have many address ranges for lease.

ibDHCPSubnetNetworkMask (IbIpAddr)
The subnet mask in dotted decimal format.

ibDHCPSubnetPercentUsed (Integer)
The percentage of dynamic DHCP addresses leased out at this time for each subnet. Fixed addresses are always counted as leased for this calculation, if the fixed addresses are within a leased address range.

Following is an example of the table as viewed through a MIB browser:

<table>
<thead>
<tr>
<th>ibDHCPSubnetNetworkAddress</th>
<th>ibDHCPSubnetNetworkMask</th>
<th>ibDHCPSubnetPercentUsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 10.0.0.0</td>
<td>255.0.0.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>2 20.0.0.0</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>3 20.0.0.00</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>4 20.0.0.00</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>5 20.0.0.00</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>6 20.0.0.00</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>7 20.0.0.00</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>8 20.0.0.00</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>9 20.0.0.00</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
<tr>
<td>10 20.0.0.00</td>
<td>255.255.255.0</td>
<td>0.0000</td>
</tr>
</tbody>
</table>

**ibDHCPStatistics**

ibDHCPStatistics maintains counters for different types of packets. The counters always start with zero when the DHCP service is restarted. Therefore, the numbers reflect the total number of packets received since the DHCP service was last restarted on the appliance. The ibDHCPStatistics module contains the following objects:

**Table 39.18 ibDHCPStatistics**

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDhcpTotalNoOfDiscovers (Counter)</td>
<td>The number of DHCPDISCOVER messages that the appliance received. Clients broadcast DHCPDISCOVER messages when they need an IP address and network configuration information.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfRequests (Counter)</td>
<td>The number of DHCPREQUEST messages that the appliance received. A client sends a DHCPREQUEST message requesting configuration information, after it receives the DHCPOFFER message.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfReleases (Counter)</td>
<td>The number of DHCPRELEASE messages that the appliance received from its clients. A client sends a DHCP release when it terminates its lease on an IP address.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfOffers (Counter)</td>
<td>The number of DHCPOFFER messages that the appliance has sent to clients. The appliance sends a DHCPOFFER message to a client. It contains an IP address and configuration information.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfAcks (Counter)</td>
<td>The number of DHCPACK messages that the appliance sent to clients. It sends a DHCPACK message to a client to confirm that the IP address offered is still available.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfNacks (Counter)</td>
<td>The number of DHCPNACK messages that the appliance sent to clients. It sends a DHCPNACK message to withdraw its offer of an IP address.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfDeclines (Counter)</td>
<td>The number of DHCPDECLINE messages that the appliance received. A client sends a DHCPDECLINE message if it determines that an offered IP address is already in use.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfInforms (Counter)</td>
<td>The number of DHCPINFORM messages that the appliance received. A client sends a DHCPINFORM message when it has an IP address but needs information about the network.</td>
</tr>
<tr>
<td>ibDhcpTotalNoOfOthers (Counter)</td>
<td>The total number of DHCP messages other than those used in negotiation, such as DHCPOFFER/RENEW, DHCPKNOWN, and DHCPLEASEQUERY.</td>
</tr>
</tbody>
</table>
ibDHCPDDNSStats

ibDHCPDDNSStats monitors the average latency for the DHCP DDNS updates in microseconds and the number of timeouts during different time intervals. The ibDHCPDDNSStats module contains the following objects:

**Table 39.19 ibDHCPStatistics**

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDHCPDDNSAvgLatency5 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCP DDNS updates in the last five minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSAvgLatency15 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCP DDNS updates in the last 15 minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSAvgLatency60 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCP DDNS updates in the last 60 minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSAvgLatency1440 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCP DDNS updates in the last 24 hours.</td>
</tr>
<tr>
<td>ibDHCPDDNSTimeoutCount5 (Integer)</td>
<td>The number of timeouts for the DHCP DDNS updates in the last five minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSTimeoutCount15 (Integer)</td>
<td>The number of timeouts for the DHCP DDNS updates in the last 15 minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSTimeoutCount60 (Integer)</td>
<td>The number of timeouts for the DHCP DDNS updates in the last 60 minutes.</td>
</tr>
<tr>
<td>ibDHCPDDNSTimeoutCount1440 (Integer)</td>
<td>The number of timeouts for the DHCP DDNS updates in the last 24 hours.</td>
</tr>
</tbody>
</table>

ibDHCPv6Module

Figure 39.14 illustrates the structure of the ibDHCPv6Module, which contains the following objects:

- ibDHCPv6SubnetTable provides statistical data about the DHCPv6 operations of the appliance. For information, see ibDHCPv6SubnetTable.
- ibDHCPv6Statistics maintains counters for different types of packets. For information, see ibDHCPv6Statistics.
- ibDHCPv6DeferredQueueSize tracks the total number of deferred DDNS updates that are currently in the queue to be retried. When DDNS updates are deferred due to timeout or server issues, the DHCP server puts these updates in this queue.
- ibDHCPv6DDNSStats monitors the average latency for the DDNS updates in microseconds and the number of timeouts during different time intervals. For information, see ibDHCPv6DDNSStats.

Figure 39.14 ibDHCPv6Module
ibDHCPv6SubnetTable

ibDHCPv6SubnetTable provides statistical data about the DHCPv6 operations of the appliance. It contains the following objects:

Table 39.20 ibDHCPv6SubnetTable

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDHCPv6Subnet Entry</td>
<td>File that contains the objects for monitoring DHCPv6 operations on the appliance.</td>
</tr>
<tr>
<td>ibDHCPv6SubnetNetworkAddress (IbIpAddr)</td>
<td>The subnetworks, in IPv6 address format, that have IPv6 addresses for lease. A subnetwork may have many address ranges for lease.</td>
</tr>
<tr>
<td>ibDHCPv6SubnetNetworkMask (IbIpAddr)</td>
<td>The subnet mask in CIDR notation format.</td>
</tr>
</tbody>
</table>

ibDHCPv6Statistics

ibDHCPv6Statistics maintains counters for different types of packets. The counters always start with zero when the DHCP service is restarted. Therefore, the numbers reflect the total number of packets received since the DHCP service was last restarted on the appliance. The ibDHCPv6Statistics module contains the following objects:

Table 39.21 ibDHCPv6Statistics

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
</table>

ibDhcpv6TotalNoOfSolicits (Counter)  The number of Solicit messages that the Grid member received, including Solicit messages embedded in Relay-Forward messages. A DHCP client sends a Solicit message to locate DHCP servers.

ibDhcpv6TotalNoOfRequests (Counter) The number of Request messages that the Grid member received. A DHCP client sends a Request message to request one or more IP addresses and configuration parameters from a DHCP server.

ibDhcpv6TotalNoOfReleases (Counter) The number of Release messages that the Grid member received. A DHCP client sends a Release message when it terminates its lease and releases its IP address.

ibDhcpv6TotalNoOfAdvertises (Counter) The number of Advertise messages that the Grid member sent. When a DHCP server receives a Solicit message, it can respond with an Advertise message to indicate that the server is available for DHCP service.

ibDhcpv6TotalNoOfReplies (Counter) The number of Reply messages that the Grid member sent. A DHCP server sends a Reply message that includes IP addresses and configuration parameters when it responds to Solicit, Request, Renew or Rebind message. It sends a Reply message with configuration parameters only when it responds to an Information-Request message.

ibDhcpv6TotalNoOfRenews (Counter) The number of Renew messages that the Grid member received. A DHCP client sends a Renew message to a DHCP server to extend the lifetimes on the leases granted by the DHCP server and to update other properties.

ibDhcpv6TotalNoOfRebinds (Counter) The number of Rebind messages that the Grid member received. A DHCP client sends a Rebind message to extend the lifetime of its lease and to update configuration parameters.

ibDhcpv6TotalNoOfDeclines (Counter) The number of Decline messages that the Grid member received. A DHCP client sends a Decline message to the DHCP server when it discovers that the IP address offered by a DHCP server is already in use.

ibDhcpv6TotalNoOfInformationRequests (Counter) The number of Information-Request messages that the Grid member received. A client sends an Information-Request message to retrieve configuration parameters, such as the IP addresses of DNS servers in the network.

ibDhcpv6TotalNoOfOthers (Counter) The total number of DHCP messages other than those used in negotiation.

ibDhcpv6DDNSStats

ibDhcpv6DDNSStats monitors the average latency for the DHCPv6 DDNS updates in microseconds and the number of timeouts during different time intervals. The ibDhcpv6DDNSStats module contains the following objects:

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibDhcpv6DDNSAvgLatency5 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCPv6 DDNS updates in the last five minutes.</td>
</tr>
<tr>
<td>ibDhcpv6DDNSAvgLatency15 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCPv6 DDNS updates in the last 15 minutes.</td>
</tr>
<tr>
<td>ibDhcpv6DDNSAvgLatency60 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCPv6 DDNS updates in the last 60 minutes.</td>
</tr>
<tr>
<td>ibDhcpv6DDNSAvgLatency1440 (Integer)</td>
<td>Indicates the average latency in microseconds of the DHCPv6 DDNS updates in the last 24 hours.</td>
</tr>
<tr>
<td>ibDhcpv6DDNSTimeoutCount5 (Integer)</td>
<td>The number of timeouts for the DHCPv6 DDNS updates in the last five minutes.</td>
</tr>
<tr>
<td>ibDhcpv6DDNSTimeoutCount15 (Integer)</td>
<td>The number of timeouts for the DHCPv6 DDNS updates in the last 15 minutes.</td>
</tr>
<tr>
<td>ibDhcpv6DDNSTimeoutCount60 (Integer)</td>
<td>The number of timeouts for the DHCPv6 DDNS updates in the last 60 minutes.</td>
</tr>
<tr>
<td>ibDhcpv6DDNSTimeoutCount1440 (Integer)</td>
<td>The number of timeouts for the DHCPv6 DDNS updates in the last 24 hours.</td>
</tr>
</tbody>
</table>

ibDNSOne MIB

The ibDNSOne MIB provides DNS statistics about all zones in all views. Figure 39.15 illustrates the structure of the ibDNSOne MIB. (Note that the
Using the DNS Zone Statistics Tables

ibZoneStatisticsTable and ibZonePlusViewStatisticsTable provide DNS statistics for all zones in all DNS views, including the default and all user-defined DNS views. You can use the information in these tables to calculate the total number of recursive queries on the DNS server. Depending on whether your DNS server is an authoritative or a caching-only server, you calculate the total number of recursive queries differently. For information, see Calculating Recursive DNS Queries.

ibZoneStatisticsTable

ibZoneStatisticsTable contains DNS statistics of all zones in the default DNS view. DNS statistics of user-defined DNS views are captured in ibZonePlusViewStatisticsTable. For information, see ibZonePlusViewStatisticsTable.

ibZoneStatisticsTable includes a "summary" zone that provides global statistics for the DNS server, including statistics for all zones in the default and user-defined DNS views.

The syntax of the objects in ibZoneStatisticsTable uses a Counter64 format. In some cases, the counter format may not be compatible with SNMP toolkits that use a 32-bit counter. Ensure that you reconfigure or update these tools to use the Counter64 format. ibZoneStatisticsTable contains the following objects:

Table 39.23 ibZoneStatisticsTable

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
</table>

Copyright ©2019, Infoblox, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibBindZonePlusViewName (IbString)</td>
<td>The zone name.</td>
</tr>
<tr>
<td>ibBindZonePlusViewSuccess (Counter64)</td>
<td>The number of successful responses since the DNS process started.</td>
</tr>
<tr>
<td>ibBindZonePlusViewReferral (Counter64)</td>
<td>The number of DNS referrals since the DNS process started.</td>
</tr>
<tr>
<td>ibBindZonePlusViewNxRRset (Counter64)</td>
<td>The number of DNS queries received for non-existent records.</td>
</tr>
<tr>
<td>ibBindZonePlusViewNxDomain (Counter64)</td>
<td>The number of DNS queries received for non-existent domains.</td>
</tr>
<tr>
<td>ibBindZonePlusViewRecursion (Counter64)</td>
<td>The number of queries that caused recursion since the DNS process started.</td>
</tr>
</tbody>
</table>

Following is an example of the table as viewed through a MIB browser:

![MIB Browser View](image)

ibZonePlusViewStatisticsTable

ibZonePlusViewStatisticsTable provides DNS statistics about all zones in user-defined DNS views. DNS statistics about zones in the default view are captured in ibZoneStatisticsTable. Note that information in ibZonePlusViewStatisticsTable is rolled up to the "summary" zone in ibZoneStatisticsTable. For information, see ibZoneStatisticsTable.

The syntax of the objects in ibZonePlusViewStatisticsTable uses a Counter64 format. In some cases, the counter format may not be compatible with SNMP toolkits that use a 32-bit counter. Ensure that you reconfigure or update these tools to use the Counter64 format.

ibZonePlusViewStatisticsTable contains the following objects:

<table>
<thead>
<tr>
<th>Table 39.24 ibZonePlusViewStatistics Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object (Type)</td>
</tr>
<tr>
<td>ibBindZonePlusViewName (IbString)</td>
</tr>
<tr>
<td>ibBindZonePlusViewSuccess (Counter64)</td>
</tr>
<tr>
<td>ibBindZonePlusViewReferral (Counter64)</td>
</tr>
<tr>
<td>ibBindZonePlusViewNxRRset (Counter64)</td>
</tr>
<tr>
<td>ibBindZonePlusViewNxDomain (Counter64)</td>
</tr>
<tr>
<td>ibBindZonePlusViewRecursion (Counter64)</td>
</tr>
</tbody>
</table>
Calculating Recursive DNS Queries

You can use the information in `ibZoneStatisticsTable` and `ibZonePlusViewStatisticsTable` to calculate the total number of recursive queries. Following is an example of `ibZoneStatisticsTable` indexed by zone names in the default view:

```
index  ibBindZoneName  ibBindZoneSuccess  ibBindZoneReferral  ibBindZoneNxRRset  ibBindZoneNxDomain  ibBindZoneRecursion  ibBindZoneFailure
"abc.com"   abc.com       0          0                  0                  0                  0
"summary"    summary      500        0                  0                  0                  0
"internal.com" internal.com  100        0                  0                  0
```

Following is an example of `ibZonePlusViewStatisticsTable` indexed by zone names in all user-defined views:

```
index  ibBindZonePlusViewName  ibBindZonePlusViewSuccess  ibBindZonePlusViewReferral  ibBindZonePlusViewNxRRset  ibBindZonePlusViewNxDomain  ibBindZonePlusViewRecursion  ibBindZonePlusViewFailure  ibBindViewName
"ext1.com"     ext1.com       100              0                  0                  0                  DNS1
"ext2.com"     ext2.com       200              0                  0                  0                  DNS1
"ext3.com"     ext3.com       0                0                  0                  0                  DNS2
```

Use the `ibBindZoneSuccess` object in both tables to determine the total number of recursive queries. If your DNS server is a caching-only server, the total number of recursive queries is the number indicated in the `ibBindZoneSuccess` object of the "summary" zone. In this example, for a caching-only server, the total number of recursive queries is 5.

If your DNS server is an authoritative server, add all the numbers in `ibBindZoneSuccess` for all zones in both tables, excluding the "summary" zone. In this example, the total is 4. You then subtract this number from the number in `ibBindZoneSuccess` of the "summary" zone. In this case, the total number of recursive queries is 1 for an authoritative DNS server.

`ibDDNSUpdateStatistics`

`ibDDNSUpdateStatistics` provides statistical data about DDNS updates. The counters always start with zero when the DNS service is restarted. They report the total numbers since the DNS service was last restarted.

`ibDDNSUpdateStatistics` contains the following objects:

<table>
<thead>
<tr>
<th>Object (Type)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ibDDNSUpdateSuccess</code> (Counter64)</td>
<td>The number of successful dynamic DNS updates.</td>
</tr>
<tr>
<td><code>ibDDNSUpdateFailure</code> (Counter64)</td>
<td>The number of all failed dynamic DNS updates, excluding those reported by the <code>ibDDNSUpdateReject</code> object.</td>
</tr>
<tr>
<td><code>ibDDNSUpdateReject</code> (Counter64)</td>
<td>The number of dynamic DNS updates that failed because they were denied by the DNS server.</td>
</tr>
<tr>
<td><code>ibDDNSUpdatePrerequisiteReject</code> (Counter64)</td>
<td>The number of dynamic DNS updates that failed because the prerequisites were not satisfied. This is also included in the total number of failures reported by the <code>ibDDNSUpdateFailure</code> object.</td>
</tr>
</tbody>
</table>
ibBindZoneTransferCount (Counter64) provides the total number of successful zone transfers from an Infoblox primary or secondary DNS server to a DNS client, since the DNS service was last restarted. Note that this counter tracks the number of successful full zone transfers (AXFRs) and incremental zone transfers (IXFRs).

**IB-DNSSERV-MIB**

The IB-DNSSERV-MIB contains one object, ibDnsServConfig, which reports the DNS BIND version implemented by the NIOS software.

**IB-DNSHITRATIO-MIB**

The IB-DNSHITRATIO-MIB contains one object, ibDnsHitRatio, which provides information about the DNS cache hit ratio. Note that the MIB variable (ibDNSOne) for cache hit rate has an OID of 1.3.6.1.4.1.7779.3.1.3.1.5.0, where 1.3.6.1.4.1.7779 is the prefix.

**IB-DNSQUERYRATE-MIB**

The IB-DNSQUERYRATE-MIB contains one object, ibDnsQueryRate, which provides information about the DNS queries per second. Note that the MIB variable (ibDNSOne) for DNS query rate has an OID of 1.3.6.1.4.1.7779.3.1.3.1.6.0, where 1.3.6.1.4.1.7779 is the prefix.

**IB-DHCPSERV-MIB**

The IB-DHCPSERV-MIB contains one object, ibDhcpv4ServerSystemDescr, which provides the DHCP server name and its DHCP version.

**Chapter 40 Infoblox Reporting and Analytics**

This chapter describes the Infoblox Reporting and Analytics solution and its features. It explains how to navigate through the user interface, view predefined dashboards, create personal reports and searches. It also provides best practices for customizing searches and setting permissions, and describes the reporting clustering feature and how to configure a reporting cluster.

It contains the following sections:

- Infoblox Reporting and Analytics
  - Upgrading from a Previous NIOS Release
  - Setting Up Reporting and Analytics
  - Supported Reporting Appliances and Storage Space
- Licensing Requirements
  - Perpetual Licensing
  - Subscription Licensing
  - About License Violations
- Administrative Permissions
  - Granting Permissions
  - Editing Permissions
- Configuring an External Server for Search Result Exports
- About Reporting Clustering
  - Clustering Overview
  - Reporting Cluster Modes
  - Clustering Data Replication
  - ReportingSite Extensible Attribute
  - Monitoring Reporting Cluster Status
  - Promoting the Grid Master Candidate in Multi-Site Clustering
  - Reporting Categories and Related Data Sources
  - Configuring Reporting Clusters
  - Assigning a ReportingSite EA Value to a Multi-Site Cluster
  - Validating Reporting Clustering Configuration
- Guidelines for Deploying Reporting Clusters
  - Best Practices for Capacity Planning
  - Monitor Volume and Storage Consumption
  - Deployment and Service Monitoring
  - Other Best Practices for Deploying Reporting Clusters
- Grid Reporting Properties
  - Configuring Grid Reporting Properties
  - Reporting (Index) Storage Space
  - Modifying Member Reporting Properties
  - Defining Interface for Reporting Traffic
  - Setting the Network Port for Reporting
  - Specifying the Data Generation Interval for Reports
  - Configuring Threat Protection Data
  - Monitoring DNS Client Queries

Copyright ©2019, Infoblox, Inc. All right reserved.
• Forwarding Syslog Data to the Reporting Server
• About IP Blocks and IP Block Groups
  • Adding IP Block Groups
  • Modifying IP Block Groups
  • Deleting IP Block Groups and IP Blocks
  • Exporting IP Block Groups and IP Blocks
  • Printing IP Block Groups and IP Blocks
• Reporting User Interface Overview
  • Home Dashboards
• About Searches
  • Creating Reports from a Search
  • Saving a Search as a Dashboard Panel
  • Exporting Search Results
  • Saving Search as Alerts
• About Alerts
  • Creating Scheduled Alerts
  • Editing Alerts
  • Cloning Alerts
  • Configuring Email Notification Settings
• About Reports
  • Reporting Indexes and Update Time Intervals
  • Cloning Reports
  • Scheduling Reports
  • Configuring Logo Image in PDF Reports
• About Dashboards
  • About Dashboard Filters
  • Creating New Dashboards
  • Cloning Dashboards
  • Resetting Dashboards
  • Editing Dashboards
  • Editing the XML Source Code of a Dashboard
  • Generate Dashboard PDFs
  • Scheduling PDF Delivery for Dashboards
• Predefined Dashboards
  • Audit Log Events
  • DHCPv4 Top Utilized Networks
  • DNS Statistics per DNS View
  • DNS Statistics per Zone
  • IPAMv4 Network Usage Statistics
  • IPAMv4 Network Usage Trend
  • IPAMv4 Top Utilized Networks
  • Inactive IP Addresses
  • Port Capacity Utilization by Device
  • Port Capacity Delta by Device
  • Port Capacity Trend
  • Port Capacity Utilization by Device
  • IP Address Inventory
  • Network Inventory
  • End Host History
  • Device Interface Inventory
  • Device Inventory
  • Device Components
  • IPAMv4 Device Networks
  • Device Class Trend
  • Device Fingerprint Change Detected
  • Device Trend
  • DHCP Lease History
  • DHCP Message Rate Trend
  • DHCP Top Lease Clients
  • DHCPv4 Range Utilization Trend
  • DHCPv4 Usage Statistics
  • DHCPv4 Usage Trend
  • Top Device Classes
  • Top Devices Denied an IP Address
  • Top Devices Identified
  • DDNS Update Rate Trend
  • DNS Cache Hit Rate Trend
  • DNS Daily Peak Hour Query Rate by Member
  • DNS Domain Query Trend
  • DNS Domain Queried by Client
  • Top DNS Clients by Query Type
  • Top DNS Clients Querying MX Records
Infoblox Reporting and Analytics

The Infoblox Reporting and Analytics solution automates the collection, analysis, and presentation of core network service data that assists you in planning and mitigating network outage risks so you can manage your networks more efficiently. It provides predefined dashboards and reports that capture useful information about the activities and performance of core network services. It also provides an enhanced reporting interface so you can create custom dashboards, reports, and alerts.

NOTE: For Reporting and Analytics to function properly, ensure that you DO NOT create a SHA-256 4096 SSL key for the HTTPS certificate in your Grid because Java does not support SHA-256 with a 4096 key size.

Through reporting clustering, you can combine and configure multiple reporting members in a cluster. These reporting members work together to provide greater performance with higher data throughput and indexing capacity. The cluster also efficiently scales storage and indexing capacity. Reporting data is replicated among these reporting appliances to ensure continuous service even if one of the servers fails. You can configure...
more reporting appliances in multiple locations (sites) so that reporting data and service can be recovered from catastrophic disasters. Thus, the reporting clustering solution increases scale, offers higher reporting performance and greatly improves the reliability of the Reporting and Analytics solution. For information about this feature, see About Reporting Clustering.

When you set up a reporting appliance with valid licenses in the Grid, the reporting server acts as an indexer that collects data from Grid members while the members are forwarders that transmit information to the reporting server. The reporting server indexes all raw data and transforms it into searchable events. Depending on your needs, you can enable certain Grid members as forwarders and disable others so the reporting server receives only the information you need from specific members. Figure 40.1 depicts the high-level configuration of the NIOS Reporting and Analytics solution:

The Infoblox reporting solution supports both IPv4 and IPv6 networks and you can configure a reporting member in IPv4, IPv6, or in dual mode (IPv4 and IPv6) network environment. An IPv4 reporting member uses IPv4 as the communication protocol, so you can add an IPv4 reporting member to an IPv4 or dual mode Grid. An IPv6 reporting member uses IPv6 as the Grid communication protocol, so you can add an IPv6 reporting member to an IPv6 or dual mode Grid. But a dual mode reporting member can use either IPv4 or IPv6 as the communication protocol, so you can add a dual mode reporting member to an IPv4, IPv6, or a dual mode Grid. For more information about how to set up the communication protocol, see Changing the Communication Protocol for a Dual Mode Appliance.

Upgrading from a Previous NIOS Release

When you upgrade from a previous NIOS release to NIOS 7.3.x and later releases, you will notice that some of the reporting features and terminologies have changed. For example, searches and reports in previous NIOS releases are now reports and dashboards respectively in the new reporting solution. In addition, your custom reports might be affected. Infoblox recommends that you take some time to explore the new user interface and get familiar with the terminologies.

You can continue to use the Infoblox predefined reports from previous releases in the new interface and customize them to meet your specific requirements, or you can create new custom reports from the ground up using a powerful search pattern.

Note: Infoblox Reporting and Analytics integrates with Splunk to deliver an enhanced reporting interface so you can create dashboards, reports, and alerts. This chapter attempts to explain all reporting functionality you can perform through the enhanced interface. However, you may need to refer to the Splunk documentation for certain functionality as indicated in specific sections of this chapter. In addition, some functions and capabilities referenced in the Splunk documentation, such as setting up custom Python scripts, are not available or applicable to the Infoblox Reporting and Analytics as some Splunk functionality in the Infoblox product may be limited or modified by Infoblox. Infoblox does not represent or warrant that Infoblox Reporting and Analytics will function in accordance with the Splunk documentation. Infoblox is also not responsible for the accuracy of the Splunk documentation. For Infoblox Reporting and Analytics technical support, contact Infoblox Technical Support. DO NOT contact Splunk.

When you upgrade from a previous NIOS release to NIOS 7.3.x and later, there are some significant changes to the Reporting and Analytics solution. Some of the important changes are as follows:

- **Terminology:** The following table lists the terminology differences when you upgrade:

<table>
<thead>
<tr>
<th>Pre-NIOS 7.3.0 Release</th>
<th>NIOS 7.3.0 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Searches</td>
<td>Reports</td>
</tr>
<tr>
<td>Reports</td>
<td>Dashboards</td>
</tr>
</tbody>
</table>

- **Object Management:** NIOS no longer manages reporting objects such as searches, smart folders, alerts, and reports. You will not be able to perform operations such as global search, quick filtering, bookmarking, and others for these objects. You can now manage these objects through the new user interface.
Note: Smart folders are migrated after an upgrade. However, data in the smart folders is not migrated, and all filters for the smart folders are reset to default.

- **Permissions**: Permissions for all reporting objects are migrated to the new Reporting and Analytics solution and managed through the new user interface after an upgrade. You may see the new built-in role. **Everyone**, when configuring Reporting permissions. For best practices, do not alter permissions for this new built-in role. Note that the Reporting Dashboard and Reporting Search global permissions have been removed. If an admin group or admin role was granted these permissions before an upgrade, the permissions will still be displayed after an upgrade. However, they won't take any effect. The Grid Reporting Properties permission is retained. In addition, reporting object permissions for dashboards and searches (including global dashboards and searches) are migrated. These object permissions are retained for applicable migrated users. If permissions were granted to a specific admin group for a dashboard or search before an upgrade, only these admin users and superusers have permissions to access the migrated dashboard and report after an upgrade. If a limited-access user group is created through the new interface after the upgrade, users in this admin group will not be able to access the dashboard and report even if they are granted access to the Infoblox Reporting and Analytics App. Superusers must explicitly grant permissions to this limited-access admin group for users in this group to access the dashboard and report. For more information, see Granting Permissions.

- **Navigation and Visualization**: Navigations for some reporting functions, such as searches, alerts, email and page settings, and email PDF delivery, have changed. You can navigate through the new user interface to get familiar with the changes in this release. In addition, all predefined reports might look different than the traditional ones depending on your filtering configuration. The Grid Reporting Properties editor and Groups tab are moved under the Administration tab –> Reporting tab.

Note: Bookmarked groups are migrated after an upgrade. The bookmarked group navigates to the Administration tab –> Reporting tab –> Groups tab.

- **Extensible Attributes**: The reports that supported filtering and grouping by multiple extensible attributes are migrated to the new interface with filtering and grouping only by the extensible attribute Site. You must clone the dashboard, add filter inputs and modify the view XML to support additional extensible attributes. For information, see Editing the XML Source Code of a Dashboard.

- **Searches and Reports**: Only NIOS system and global reports and searches are migrated to NIOS 7.3.0 and later versions as dashboards and reports respectively. All user private reports and searches are dropped. In addition, bookmarked reports and searches are not migrated to 7.3.x release. If you want to keep any customization for the user private dashboards and reports, do one of the following:
  - Create global dashboards and reports using the same settings.
  - After an upgrade, you can clone the corresponding migrated system or global dashboards and reports, and then reconfigure the original settings, such as filters and scheduling in the new user interface.

- **Custom Search**: You can create your own search pattern and save it as a dashboard or report. For information, see About Searches.

After completing the NIOS upgrade successfully, you configure the Grid Reporting properties and remote server (FTP, SCP, or TFTP) to export search results. For information, see Configuring Grid Reporting Properties and Configuring an External Server for Search Result Exports.

### Setting Up Reporting and Analytics

To enable and start using the Infoblox reporting solution on supported reporting appliances, complete the following:

1. Install a valid Reporting license on the reporting appliance, as described in Licensing Requirements. Note that Infoblox now offer subscription licenses for the reporting solution.
2. Set administrative permissions, as described in Administrative Permissions.
3. Configure reporting properties, as described in Grid Reporting Properties.
4. Start the reporting service on the indexer and forwarders.

### Supported Reporting Appliances and Storage Space

Infoblox provides several reporting appliances to address different reporting requirements. Table 40.3 lists the supported Trinzic Reporting platforms based on IP capacities and average DHCP leases and DNS queries per second. There will be an impact on the performance of your reporting server when you perform many searches, download PDF reports, and send reports through emails and alerts. It is important to consider the reporting server configuration and make sure that it can handle the overall workload. A reporting appliance uses up to 95% of the total reporting disk space. The usable hard disk space on different appliance models is shown in Table 40.2.

**Table 40.2 Infoblox Reporting Appliances and their Usable Reporting Hard Disk Space**

<table>
<thead>
<tr>
<th>Enterprise Model</th>
<th>Supported Infoblox Model</th>
<th>Reporting Hard Disk Space</th>
<th>Usable Reporting Hard Disk Space (GB)</th>
<th>Daily Maximum Data Consumption*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trinzic Reporting 5005 Appliance (User-configurable)</td>
<td>IB-V5005</td>
<td>User-defined hard disk space</td>
<td>User-defined hard disk space</td>
<td></td>
</tr>
<tr>
<td>Very Large enterprises Service providers - Trinzic Reporting 4000 Appliance</td>
<td>IB-4000 (8x300GB HDD)</td>
<td>1555 GB</td>
<td>1477</td>
<td>20 GB</td>
</tr>
<tr>
<td></td>
<td>IB-VM-4000</td>
<td>1500 GB</td>
<td>1477</td>
<td>20 GB</td>
</tr>
</tbody>
</table>
### Licensing Requirements

You can install a valid Reporting license on a supported Trinzic Reporting platform and configure it as a reporting member solely for reporting purposes. You cannot add licenses to run other services, such as DNS and DHCP, on the reporting member. For information about Infoblox platforms that support reporting, see About Reporting Clustering.

Infoblox offers perpetual and subscription licensing programs to meet your business needs. You must obtain a new replacement license from Infoblox if you want to transfer an existing license to another member.

#### Perpetual Licensing

A perpetual license is appliance-specific, meaning you can install only one perpetual license on each reporting appliance. There is no expiration date for this license type and you can use the Infoblox Reporting service for the lifetime of the appliance. However, you cannot install a perpetual license on an appliance that already has a valid DNS, DHCP, Microsoft Management, Query Redirection, or Multi-Grid Management license installed. You also cannot join a reporting member that has a perpetual license to a Grid that has a subscription license installed. A subscription license is a Grid-wide license and is not appliance-specific. Reporting members that have perpetual licenses can join a Grid that does not have a subscription license. For information about subscription licenses, see Subscription Licensing.

**Note:** All reporting appliances come with a 500 MB trial license. You can use the set temp_license CLI command to install the trial license. Available indexing capacity for a perpetual license: 1, 2, 5, 10 and 20 GB.

If you plan to configure reporting clustering, note that the overall indexing capacity for a reporting cluster increases based on the total licensing capacity for all reporting members. For example, if your Grid has three reporting members with 2 GB licensing capacity each, the overall cluster indexing capacity for the cluster becomes 6 GB. However, the stacking indexing capacity does not apply to trial licenses. In other words, if the three reporting members in your Grid all have trial licenses, the total cluster indexing capacity remains at 500 MB. For information about reporting clustering, see About Reporting Clustering.

Note that you cannot install a perpetual reporting license on a Grid that has unrestricted reporting VMs as Grid members and vice versa.
However, you can install a subscription license on a Grid that has unrestricted reporting VMs as Grid members. Unrestricted reporting VMs are reporting appliances for which you can arbitrarily configure CPU, memory, and disk size. You can arbitrarily configure CPU, memory, and disk size on IB-V5005 appliance.

Subscription Licensing

A subscription license is a Grid-wide license that you install on the Grid Master, and it is not appliance-specific. A subscription license can either be permanent or have an expiration date and Grid Manager (the Infoblox GUI) displays a 90-day and 30-day warning prior to the actual expiration date. The effective start date for a subscription license starts on the day you generate the license. Note that a reporting member that has a perpetual license is not allowed to join the Grid that has a subscription license. In a dynamic license pool, expiration warnings are based upon the expiration dates of the sub pools. When any licenses in a sub pool expire, the total available licenses for a pool drops accordingly. On the other hand, a perpetual static license allocated to an appliance does not expire. The appliance continues to run the feature for the lifetime of that appliance. For more information about Grid-wide licenses, see Managing Grid-wide Licenses.

Note: Available indexing capacity for a subscription license: 1, 2, 5, 10, 20, 50, 100, 200, and 500 GB. Contact your Infoblox representative for pricing and availability information.

About License Violations

License violations occur when the reporting appliance exceeds the maximum allowed daily volume or when the indexed data type is not allowed for the license type. There might be an impact on the reporting service performance if violations occur. License violation is reported in the Reporting tab of Grid Manager. During the license violation period, the reporting server continues to index data but the search function will cease to be operational. This means that the Reporting tab is available with the following warning message displayed: "Reporting Service is unavailable." You can apply a Reset license to remove the violations. Contact Infoblox Technical Support to obtain a Reporting Reset license. Note the following behavior for such violations:

- NIOS continues to index data; however, you will not be able to use the search feature.
- You can use the reporting search when the number of violations in the previous 30 days is within the limit. To obtain valid licenses, contact your Infoblox representative or Infoblox Technical Support.
- If there are five consecutive violations in five consecutive days, then the search feature is disabled for the next 25 days until a Reset license is installed. If necessary, contact Infoblox Technical Support to obtain a Reporting Reset license so you can reset the current license violations.
- When a license violation, summary indexing does not work and reports that use the summary index will not display output. For information about reports that use the summary index, see Summary Indexes.

Administrative Permissions

You must have the appropriate permissions to access, view, edit, and clone searches, dashboards, reports, and alerts that are available in the Reporting tab. NIOS synchronizes all users and admin groups as users and roles on the reporting server. In NIOS, admin groups may have the setting "superusers" enabled or disabled. NIOS groups that have "superusers" enabled will correspond to roles with administrative permissions on the reporting server. This documentation will refer to this role as a superuser role and the associated users as superusers. NIOS groups that do not have "superusers" enabled will not have administrative permissions on the reporting server. This role will be referred to as a non-superuser role and the associated users are limited-access users. The default NIOS admin group "admin-group" will have a superuser role on the reporting server called "infoblox-admin-role." The default NIOS admin named "admin" will have a user name on the reporting server called "infoblox-admin."

Note: When you enable the reporting service, the splunk-reporting-group is created automatically for authentication by the Reporting and Analytics App on the Grid. It is an internal admin group, so you must not add users to this group or rename it.

By default, superusers have full access to the Reporting and Analytics App and limited-access users do not. Superusers can grant permissions to limited-access users so they can access the Reporting and Analytics App. Limited-access users will not have access to the Reporting tab until superusers grant them this access. For information about Splunk roles, refer to the Splunk documentation. Note that the reporting service does not support non-ASCII characters in the names of admin groups and admin users. When you include ASCII characters and space in the admin user name, make sure that its length does not exceed 33 characters.

When configuring NIOS, only superuser and users with the Grid Reporting Properties permission can configure Grid Reporting Properties. Limited-access users can view the Grid Reporting Properties. When superusers create or delete any admin groups in NIOS, the corresponding roles are created or deleted on the reporting server. You cannot directly create or delete roles on the reporting server. If superuser permission is granted or removed from a NIOS group, this permission change will be reflected in the corresponding role on the reporting server. When you modify the name of an admin group on NIOS, make sure that you grant permissions again for all corresponding roles that are created on the Reporting and Analytics App for this renamed admin group. For information about granting permissions, see Granting Permissions.

Note: Limited-access users cannot create, modify, and delete any user role for the Splunk App.

Granting Permissions
Superusers can grant App permissions to limited-access users. Permissions for all reporting objects are migrated to the new Reporting solution and managed through the new user interface after an upgrade. You may see some new built-in roles, such as Everyone, when configuring Reporting permissions. For best practices, do not alter permissions for these new built-in roles. In addition, Reporting Dashboard and Reporting Search global permissions have been removed. If an admin group or admin role was granted these permissions before an upgrade, the permissions will still be displayed after an upgrade. However, they won't take any effect. The Grid Reporting Properties permission is retained.

**Note:** The App Permissions and Edit Permissions sections display only your assigned admin role on the reporting server. Therefore, you can only view the admin role to which your user name was assigned. Only the default system admin can view all admin roles.

To set permissions:

1. From the **Reporting** tab -> select the **Administration** tab.
2. Click **Permission** to manage permissions.
3. In the **App Permissions**, set permissions to **Read** and/or **Write** for the roles listed. You must have at least one permission (Read or Write) to execute a task on the **Reporting** tab.
4. Click **Save**.

**Figure 40.2 Setting Permissions for Reporting and Analytics App**

To modify permissions:

1. From the **Reporting** tab -> select **Dashboards** or **Reports** or **Alerts**.
2. From the **Edit** drop-down list, select **Edit Permissions**.
3. Specify the following:
   - Display for **Owner**, **App**, or **All Apps**. For more information about **All Apps** permissions, refer to the Splunk documentation.
   - Read and write privileges for users. By default, the permissions are set on the object. You cannot remove the Read and Write permissions completely. However, you can change this permissions from **Read** to **Write** or vice versa, based on your permissions. For more information about permissions, refer to the Splunk documentation.
4. Click **Save**.

Editing Permissions

Users can edit permissions for objects where they are the owner, such as dashboards, reports, and alerts. When a user creates a new report, dashboard or an alert, it is only available to that user. To make that object available to other users, you can do the following (only if your permissions allow you to do so):

- Make an object available to all users.
- Restrict or expand access to all or specific objects by roles.
- Set Read or Write permissions at the Reporting level for roles. For information about users and roles, refer to the Splunk documentation.
Configuring an External Server for Search Result Exports

You can configure an FTP, SCP, or TFTP server to which you plan to schedule the export of search results. Only superusers can configure the remote server and limited-access users cannot do so. When you upgrade to 7.3.x, make sure that you reconfigure an FTP, SCP, or TFTP server, even if you have already scheduled the export of search results. The Set up page to configure an FTP, SCP, or TFTP server is displayed for all new installations and upgrades if you have not previously scheduled the export of search results. If you have configured any scheduled export of search results in a previous NIOS release, NIOS migrates one of the server settings to the Reporting and Analytics App. In this case, the Set up page from the Reporting tab > Administration tab, as illustrated in Figure 40.3.

To configure an FTP, SCP, or TFTP server:

1. From the Reporting tab -> select the Administration tab -> click Set up.
2. To configure a remote server, complete the following:
   - **Username**: Enter the username of your server account.
   - **Password**: Enter the password of your server account.
   - **Confirm Password**: Enter the same password.
   - **Protocol**: Select FTP or SCP or TFTP from the drop-down list.
   - **Host/IP Address**: Enter the host IP address.
   - **Host Port**: Enter the port number on the selected server.
   - **Destination Path**: Enter the path and the file name of the export file. For example, you can enter /export/Infoblox_2009_10_20_15_30 on a Linux server, or c:/export/Infoblox_2009_10_20_15_30 on a Microsoft Windows server.
3. Click Save.

Figure 40.3 Setup Page to specify Server for Exporting Search Results

About Reporting Clustering

You can add higher scale, performance, and reliability to the Reporting and Analytics solution by using the reporting clustering feature. Through reporting clustering, you can combine and configure multiple reporting members in a cluster. These reporting members work together to provide greater performance with higher data throughput and indexing capacity. The cluster efficiently scales storage and indexing capacity. The reporting clustering feature also offers high availability and disaster recovery. You can configure one or more reporting appliances in multiple locations (sites). Reporting data is replicated among these reporting appliances to ensure redundancies and continuous service even if one of the servers fails. For example, if one of the reporting members has operational issues, reports and dashboards will use backup copies of the data on other reporting members in the cluster to ensure continuous reporting service. When a new reporting member joins the cluster, you do not need to reconfigure and restart your forwarders to send data to the new reporting member as the Grid Master automatically notifies all forwarders about
the new member. In addition, data indexed on the new reporting member participates in searches that support reports and dashboards. Thus, the new reporting clustering solution increases scale, offers higher reporting performance and greatly improves the reliability of the Reporting and Analytics solution.

The reporting clustering feature is supported on appliances running NIOS version 7.3.200 and later. For new installations and upgrades from a previous NIOS release to NIOS 7.3.200 and later, the appliance is set to the single indexer mode by default. For more information about how reporting clustering works and the types of clustering mode, see Clustering Overview and Reporting Cluster Modes.

**Note:** Reporting clusters are not supported in a Multi-Grid configuration.

### Clustering Overview

The concept of reporting clustering is to set up a group of reporting members within one site (location) or across multiple sites. When you configure multiple reporting members within one site, you are setting up a single-site cluster. Configuring multiple reporting members across different sites gives you a multi-site cluster, as illustrated in Figure 40.6. Single-site clusters and multi-site clusters provide scalability for storage and indexing capacity. They also offer the benefits of high availability and disaster recovery. Without reporting clustering, a reporting member is known as a single indexer.

A reporting cluster, either single-site or multi-site, consists of the following components that work together to perform reporting and clustering activities:

- **Cluster Master:** The cluster master coordinates all clustering activities and always runs on the Grid Master.
- **Indexer** (also known as cluster peer): An indexer that collects, processes, and indexes reporting data. It can also function as the originating indexer (source peer) or a replication target (target peer).
- **Forwarder:** A forwarder sends reporting data to the indexer for processing.
- **Search Head:** A search head handles search queries and distributes search requests to indexers in the cluster. One of the reporting members in the cluster will have double duties of being the indexer and search head.
- **Replication Factor:** This factor defines the number of copies of reporting data the cluster replicates and maintains. This is set to 2 by default for both single-site and multi-site clusters so the clusters can tolerate one reporting member failure without losing any data (since there will still be another copy of data available in the cluster).
- **Search Factor:** This factor defines the number of copies of searchable data. This is set to 2 for single-site clusters and set to 1 for multi-site clusters so the cluster can tolerate one reporting member failure without impacting search results (since there will still be a searchable copy of data available in the cluster).
- **ReportingSite Extensible Attribute:** This is an extensible attribute that you associate with reporting members in a multi-site cluster. For more information, see ReportingSite Extensible Attribute.

In a Grid that includes a reporting cluster, the Grid Master coordinates various activities across reporting members. In the reporting cluster, a reporting member can act as an indexer and/or a search head. It also participates in peer-to-peer data replication.

To configure a reporting cluster, you must first set up all the reporting members and enable the reporting service in the Grid. You can then select the reporting clustering type for your cluster. For more information about cluster types, see Reporting Cluster Modes. When you configure the reporting cluster, you must use an NTP server to synchronize the time of the Grid Master, Grid members, and reporting members.

### Reporting Cluster Modes

You must first enable the reporting service and configure one or more reporting members as needed before configuring the reporting cluster. When you enable reporting clustering, the Grid Master, forwarders, and reporting members use specific ports for network communication. Figure 40.4, Figure 40.5, and Figure 40.7 illustrates whether the network communication is over TCP/SSL or VPN, and ports that you can use for the reporting service.

- **Single Indexer:** This is the traditional configuration that works on one reporting server (indexer). The forwarder sends reporting data to the indexer and the indexer indexes the data. This is the default configuration when you enable the reporting service for new installations and when you upgrade from a previous NIOS release to NIOS 7.3.200 and later.

*Figure 40.4 Ports Required for IPv4 and IPv6 Single Indexer*
**Single-Site Cluster**: In a single-site cluster, the Grid Master is also the cluster master and all reporting members are cluster indexer peers. NIOS selects a peer and configures it as the search head to handle search queries. If the selected search head goes down, NIOS automatically selects another search head among the reporting members in the same site. All other Grid members (non-reporting members) are considered forwards that send reporting data to the cluster peers for processing. You must configure at least two reporting members that are located in the same site (location). By default, the replication factor and search factor for a single-site cluster are set to 2. Note that you can upgrade your configuration from a single-site cluster to a multi-site cluster. However, once configured, you cannot change your configuration back to a single indexer. For information about how to configure a single-site cluster, see Configuring Reporting Clusters.

**Multi-Site Cluster** - A multi-site clustering configuration is useful when you want to manage multiple reporting sites at different locations, with each site having its own set of indexers. The multi-site clustering configuration is valid only when you associate all the reporting members in the cluster with the predefined ReportingSite extensible attribute. For information about the ReportingSite extensible attribute, see ReportingSite Extensible Attribute. In a multi-site cluster, you configure one of the sites as the primary site, and then plan other sites in a specific order. This order defines the next site of indexers to which the forwards send data when the primary site is out of service. Note that all Grid members send data only to indexers in the primary site. You can designate a new primary site either by using the Grid Reporting Properties editor, or using the set promote_master CLI command. For more information about the CLI command, refer to the Infoblox CLI Guide. A multi-site cluster must have at least two sites with two reporting members in each site, as
The first reporting site that you configure is the primary site, which also hosts the search head for the cluster. If the search head goes down, the Grid Master automatically chooses an available reporting member in the same site as the search head. If all the indexers in a site go down, or if you want to change the search head to another site, then you must manually redefine the primary site. Note that you must make one of the active sites as the primary site. In a multi-site cluster, the search factor (also known as the site search factor) determines both the number of searchable copies that the entire cluster maintains and the number of copies that each site maintains. By default, the search factor is set to 1 and the replication factor is 2 in a multi-site cluster.

**Note:** You can change your configuration from a single indexer to a single-site cluster or multi-site cluster and from a single-site cluster to a multi-site cluster. However, you cannot revert your configuration from a multi-site cluster to a single-site cluster or to a single indexer.

### Clustering Data Replication

When you change the configuration from a single indexer to a single-site cluster or multi-site cluster and from a single-site cluster to a multi-site cluster, the replication of data will start only for the new data that are created after you have completed the cluster mode configuration. When you change the configuration, the replication of new data starts only after you have completed the clustering configuration. Any data created prior to switching are restored on the primary site and are not replicated on the secondary site. To manage your reporting clustering data efficiently, see [Guidelines for Deploying Reporting Clusters](http://docs.splunk.com/Documentation/Splunk/6.2.5/Indexer/Basicclusterarchitecture).

**Figure 40.6 Sample Multi-Site Reporting Cluster**

![Diagram of a multi-site reporting cluster](image)

**Master Control Coordinator**
---

**Search Request Results**
---

**Replication (Indexer Data and Searchable Copier)**
---

**Forwarded Data**
---

For more information about how reporting cluster works, refer to the Splunk documentation at [http://docs.splunk.com/Documentation/Splunk/6.2.5/Indexer/Basicclusterarchitecture](http://docs.splunk.com/Documentation/Splunk/6.2.5/Indexer/Basicclusterarchitecture).

**Figure 40.7 Port Requirement for IPv4 and IPv6 Multi-site Clustering**
ReportingSite Extensible Attribute

NIOS defines the ReportingSite extensible attribute for use by the multi-site cluster reporting configuration. You must associate a ReportingSite extensible attribute value with the reporting members defined in the cluster. For more information, see Assigning a Reporting Site EA Value to a Multi-Site Cluster. Note that your multi-site cluster configuration is invalid unless you assign ReportingSite values to all the reporting members that are part of the cluster.

You can add up to five ReportingSite extensible attributes, and view and edit the ReportingSite extensible attributes in the Administration tab -> Extensible Attributes tab in Grid Manager. You can view the ReportingSite extensible attribute values in the Grid -> Grid Manager -> Members tab in Grid Manager. The ReportingSite column is not available if you customize the Results table. You can enable the ReportingSite column by selecting Columns -> Edit Columns. For information, see Customizing Tables. You can also use the Group Results function to group reporting members that contain the same ReportingSite extensible attributes. For information about grouping members by extensible attributes, see Grouping Members by Extensible Attributes.

As illustrated in Figure 40.6, the ReportingSite value "site1" is assigned to a site within a multi-site cluster and to the reporting members RM1, RM2 and RM3. The ReportingSite value "site2" is assigned to a different site in the cluster and to reporting members RM4, RM5 and RM6. If the search head goes down, the Grid Master automatically chooses an available reporting member in the same site to be the search head.

Note: When you modify the ReportingSite extensible attribute value for any indexers in a multi-site cluster, ensure that you validate the configuration again, as described in Validating Reporting Clustering Configuration.

Monitoring Reporting Cluster Status

After you have set up reporting members and defined clustering type, you can monitor the cluster status through the following:


- View the reporting member service status, as described in Monitoring Grid Services.
- Check license usage by the reporting member, as described in Home Dashboards.

### Promoting the Grid Master Candidate in Multi-Site Clustering

If the Grid Master fails and all other reporting members are up and running in a multi-site reporting cluster, you must promote the Grid Master Candidate to the Grid Master by using the CLI command set promote_master. For information about the CLI command, refer to the Infoblox CLI Guide.

### Reporting Categories and Related Data Sources

The reporting member uses two types of data sources to generate reports: file-based data sources and script-based data sources. When the reporting member is down or unreachable, file-based data sources are queued until the reporting member is up and running. However, the script-based data sources are lost if the size of the queued data exceeds 500 KB.

The amount of data in the queue is managed as follows:

- Rotates the reporting syslog files (extracted from /var/log/messages) at 120 MB retaining one older file. The data in the queue depends on the file size when the reporting member becomes unreachable.
- The CSV files overwrite the oldest data with the new data at regular intervals. So, the CSV file contains only the latest events.

Table 40.3 lists the reports provided by the reporting server, report categories, and the source type, data source type (file or script-based), and queue data update frequencies for each report:

<table>
<thead>
<tr>
<th>Report Category</th>
<th>Reports</th>
<th>Source Type</th>
<th>Data Source Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Inactive IP Addresses</td>
<td>ib:reserved2</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>Port Capacity Utilization by Device</td>
<td>ib:reserved2</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>Port Capacity Trend</td>
<td>ib:reserved2</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>Port Capacity Delta by Device</td>
<td>ib:reserved2</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>End Host History</td>
<td>ib:discovery:end_host_activity</td>
<td>file</td>
</tr>
<tr>
<td>DHCP Performance</td>
<td>DHCP Message Rate Trend</td>
<td>ib:dhcp:message</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>DHCPv4 Usage Trend</td>
<td>ib:dhcp:range</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>DHCPv4 Range Utilization Trend</td>
<td>ib:dhcp:range</td>
<td>file</td>
</tr>
<tr>
<td>DHCP Lease History</td>
<td>DHCP Lease History</td>
<td>ib:dhcp:lease_history</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>DHCP Top Lease Clients</td>
<td>ib:dhcp:lease_history</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>Top Devices Identified</td>
<td>ib:dhcp:lease_history</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>Device Trend</td>
<td>ib:dhcp:lease_history</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>Device Class Trend</td>
<td>ib:dhcp:lease_history</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>Top Device Classes</td>
<td>ib:dhcp:lease_history</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>Top Devices Denied an IP Address</td>
<td>ib:dhcp:lease_history</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>Device Fingerprint Change Detected</td>
<td>ib:dhcp:lease_history</td>
<td>file</td>
</tr>
<tr>
<td>DNS Performance</td>
<td>DNS Response Latency Trend</td>
<td>ib:dns:perf</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>DNS Effective Peak Usage Trend for Flex Grid License</td>
<td>ib:dns:perf</td>
<td>scr</td>
</tr>
<tr>
<td>DNS Record Scavenging</td>
<td>DNS Scavenged Object Count Trend</td>
<td>ib:dns:reclamation</td>
<td>file</td>
</tr>
<tr>
<td>DNS Query Capture</td>
<td>DNS Domain Query Trend</td>
<td>ib:dns:capture</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>DNS Domains Queried by Client</td>
<td>ib:dns:capture</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>Top DNS Clients by Query Type</td>
<td>ib:dns:capture</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>Top DNS Clients Querying MX Records</td>
<td>ib:dns:capture</td>
<td>file</td>
</tr>
<tr>
<td>DDNS</td>
<td>DDNS Update Rate Trend</td>
<td>ib:ddns</td>
<td>file</td>
</tr>
<tr>
<td>DNS Traffic Control</td>
<td>DNS Traffic Control Resource Availability Trend</td>
<td>ib:dns:reserved</td>
<td>file</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------</td>
<td>----------------</td>
<td>------</td>
</tr>
<tr>
<td></td>
<td>DNS Traffic Control Resource Availability Status</td>
<td>ib:dns:reserved</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>DNS Traffic Control Resource Pool Availability Trend</td>
<td>ib:dns:reserved</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>DNS Traffic Control Resource Pool Availability Status</td>
<td>ib:dns:reserved</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>DNS Traffic Control Response Availability Status Distribution Trend</td>
<td>ib:dns:reserved</td>
<td>file</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DDI Utilization</th>
<th>DHCPv4 Usage Statistics</th>
<th>ib:dhcp:network</th>
<th>file</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DHCPv4 Top Utilized Networks</td>
<td>ib:dhcp:network</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>IPAM Network Usage Top Networks</td>
<td>ib:ipam:network</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>DNS Zone Statistics Per DNS View</td>
<td>ib:dns:view</td>
<td>file</td>
</tr>
<tr>
<td></td>
<td>DNS Statistics per Zone</td>
<td>ib:dns:zone</td>
<td>file</td>
</tr>
</tbody>
</table>

| IPAM Utilization | DNS Object Count Trend for Flex Grid License | ib:dns:summary | file |

<table>
<thead>
<tr>
<th>System Utilization</th>
<th>CPU Utilization Trend</th>
<th>ib:system</th>
<th>scr</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Memory Utilization Trend</td>
<td>ib:system</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>Traffic Rate by Member</td>
<td>ib:system</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>License Pool Utilization</td>
<td>ib:system</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>Flex Grid Licensing Features Enabled</td>
<td>ib:system</td>
<td>scr</td>
</tr>
</tbody>
</table>

| System Capacity | System Capacity Prediction | ib:system_capacity:objects | scr |

<table>
<thead>
<tr>
<th>DNS Query</th>
<th>DNS Replies Trend</th>
<th>ib:dns:stats</th>
<th>scr</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DNS Cache Hit Rate Trend</td>
<td>ib:dns:query:cache_hit_rate</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>DNS Query Rate by Query Type</td>
<td>ib:dns:query:qps</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>DNS Query Rate by Member Daily Query Rate by Member</td>
<td>ib:dns:query:by_member</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>DNS Daily Query Rate by Member</td>
<td>ib:dns:query:by_member</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>DNS Top Clients</td>
<td>ib:dns:query:top_clients</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>DNS Top Requested Domain Names</td>
<td>ib:dns:query:top_requested_domain_names</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>DNS Top Clients Per Domain</td>
<td>ib:dns:reserved</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>DNS Top NXDOMAIN / NOERROR (no data)</td>
<td>ib:dns:reserved</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>DNS Top SERVFAIL Errors Received</td>
<td>ib:dns:reserved</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>DNS Top SERVFAIL Errors Sent</td>
<td>ib:dns:reserved</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>DNS Top Timed-Out Recursive Queries</td>
<td>ib:dns:reserved</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>DNS Query Trend per IP Block Group</td>
<td>ib:dns:reserved</td>
<td>scr</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security</th>
<th>DNS Top RPZ Hits</th>
<th>ib:dns:reserved</th>
<th>scr</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DNS Top RPZ Hits by Clients</td>
<td>ib:dns:reserved</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>Top DNS Firewall Hits</td>
<td>ib:dns:reserved</td>
<td>scr</td>
</tr>
<tr>
<td></td>
<td>Malicious Activity by Client</td>
<td>ib:dns:reserved</td>
<td>scr</td>
</tr>
</tbody>
</table>
Configuring Reporting Clusters

You can configure a reporting single indexer, a single-site cluster, or a multi-site cluster. When you configure reporting clustering, make sure that you configure two or more reporting appliances and that all indexers are online.

Note: There is no action required if you see intermittent “Too many streaming errors” and “Skip indexing” messages in the Messages menu of the Reporting tab. This can be caused by network connectivity issues between the reporting nodes.

To configure a reporting cluster:

1. From the Administration tab -> Reporting tab, click Grid Reporting Properties from the Toolbar.
2. In the Grid Reporting Properties editor, select the Reporting Clustering tab and complete the following:
   - **Single Indexer**: Select this to configure only one reporting server. This is the default reporting cluster mode.
   - **Single-Site Cluster**: Select this if you want to configure two or more reporting servers in the same site (location). The data is replicated on multiple reporting servers. You can upgrade your configuration to the multi-site clustering mode, but you cannot revert this configuration to a single indexer mode.
   - **Multi-Site Cluster**: Select this if you want to configure multiple reporting servers at different sites (locations). You must assign the ReportingSite extensible attributes to all the reporting members that you have configured in the same site within the cluster. You can configure the same ReportingSite extensible attribute with multiple reporting members. The reporting members that are configured with the same ReportingSite extensible attributes are tagged to the same site. Click the Add icon and select the ReportingSite extensible attribute that you have configured on the reporting member. The first site that you add is considered to be the primary site, which functions as the search head. You can change the order of the sites by clicking the up and down arrows.

   For more information about the reporting cluster type, see Reporting Cluster Modes.

Note: Your multi-site configuration is invalid if you do not add the correct ReportingSite extensible attribute values to the reporting members. You can validate your configuration as described in Validating Reporting Clustering Configuration.

3. Click Save & Close.

Assigning a ReportingSite EA Value to a Multi-Site Cluster

The multi-site clustering configuration is valid only when you associate all the reporting members in the cluster with the specified ReportingSite e
xtensible attribute values. Make sure that you select the ReportingSite values from those that are specified for the multi-site cluster in the Grid Reporting Properties editor. After you assign extensible attribute values to the reporting members, you can validate the multi-site cluster configuration as described in Validating Reporting Clustering Configuration.

To associate the ReportingSite extensible attribute with the reporting member:

1. From the Grid tab, select the Grid Manager tab -> Members tab -> member check box, and then click Extensible Attributes in the Toolbar.
2. Click the Add icon in the Extensible Attributes table to enter extensible attributes. The appliance adds a row to the table each time you click the Add icon. Select the row and the attribute name from the drop-down list, and then enter the value.
3. Optionally, select an extensible attribute and click Delete to delete it.
4. Click Save & Close.

Validating Reporting Clustering Configuration

After you have configured the reporting cluster mode, you can verify its validity. Whenever you make changes to the reporting configuration through Grid Manager or hardware replacement, make sure that you validate the configuration.

When you verify a multi-site cluster configuration, NIOS validates the following:

- The extensible attribute ReportingSite is specified for all reporting members.
- The set of extensible attributes configured in the GridReportingProperties editor equals to the set of ReportingSite extensible attributes defined for the reporting members.
- For each ReportingSite extensible attribute, the number of reporting peers must be greater or equal to the replication factor in each site.
- For each ReportingSite extensible attribute, the search factor must be less than or equal to the replication factor in each site.

To verify the reporting cluster-mode configuration:

1. From the Grid tab -> Grid Manager tab, click the Reporting service.
2. In the vertical Toolbar, click Verify Cluster Configuration.
   The Verify Reporting Cluster Configuration dialog box displays an error message if the configuration is invalid. Make sure that you associate the ReportingSite extensible attributes with all the reporting members that you have configured.
3. Click OK to close the dialog box.

Guidelines for Deploying Reporting Clusters

The following are a few guidelines to consider before you deploy reporting clustering:

- **Best Practices for Capacity Planning**
- **Monitor Volume and Storage Consumption**
- **Deployment and Service Monitoring**
- **Best Practices for Customizing Searches**

Best Practices for Capacity Planning

- Forecast the usage of the reporting volume and disk size based on your business needs and estimate the future potential growth.
- Work with the your Infoblox representatives to gather statistics and metrics of your Grid to estimate the expected potential reporting data volume and disk storage required to manage your reporting data. This helps you determine which tier of NIOS Reporting license you should purchase, the number of appliances, and the appliance models you might need.
- Configure reporting appliances using the same hardware appliance models. The capacity of the whole cluster is limited by the weakest reporting member if you configure reporting members using different appliance hardware models.
- Consider the future potential growth during the initial deployment of a reporting cluster. Scaling out the reporting cluster by adding more reporting members at a later time might result in a significant configuration change.
- Unlike single-indexer reporting solution, there might be more than one solutions to handle certain estimated license and disk size for the reporting cluster. To reduce the potential admin overhead, Infoblox recommends that you use a small number of high-end reporting appliances to form a cluster, rather than using a large number of low-end reporting appliance.
- When deploying a reporting cluster in a virtual environment, consider the following:
  - You can deploy clustering in a virtual environment as long as it provides adequate system resources and capacities. Refer to the following resources to help design the clustering deployments. They provide information about best practices and consequences that you should be aware of when configuring the host environments:
    - http://docs.splunk.com/Documentation/Splunk/6.3.3/Capacity/Referencehardware
    - https://www.splunk.com/web_assets/pdfs/secure/Splunk_and_VMware_VMs_Tech_Brief.pdf
    - https://answers.splunk.com/answers/238/can-i-run-splunk-in-a-vm-are-there-any-issues-or-tricks-i-should-be-aware-of.html
  - If you expect to deploy the reporting cluster in multiple data centers to achieve disaster recovery in the future, then configure the multi-site reporting clustering for the first time, even if all reporting members are physically located in the same data center. You can move some of the reporting members to other data center at a later time as required, rather than deploying new reporting members and reconfiguring the multi-site cluster.

**Note:** Be aware that the additional reporting members (the secondary site in the same data center) doesn't really increase the capacity of the
• Reporting cluster can only tolerate single node failure.
  • By default, the replication factor is set to 2, which means that there are two copies for each bucket in the entire single-site cluster or each site for a multi-site cluster. Therefore, it can tolerate failure only on one node.
  • The cluster may not be able to tolerate double failure. For example, if node1 just recovered from a failure and if node2 fails before node1 is fully recovered (before turning everything to green). In such cases, there is a chance of losing some data.
  • When you change the reporting cluster mode, be aware of the following:
    • The data indexed by a single-indexer is not replicated to other peers, even if upgraded to a single-site cluster. Similarly, the data indexed by a single-site cluster is not replicated to other sites, even if upgraded to a multi-site cluster. In other words, the single-indexer configuration does not support HA configuration and single-site data does not have disaster recovery measure. Note that when you restore the reporting data created in a single-site cluster to a multi-site cluster, the data is restored only on the primary site of the cluster and are not replicated on the secondary site.

Monitor Volume and Storage Consumption

• Monitor the license volume usage on the reporting server regularly using the following dashboards:
  • Monitor the Today’s License Usage (GB) and License Usage Trend Per Member panels available in the Home Dashboards
  • Reporting License Usage
  • Reporting Volume Usage Trend per Category
  • Reporting Volume Usage Trend per Member
• Configure alerts in the Infoblox Reporting and Analytics App to trigger actions when data volume reaches a specified limit.
• Monitor the disk usage: You can monitor the disk usage for each index in the Grid Reporting Properties editor and adjust the breakdown among indexes to make sure that the data is retained for the desired period of time.
• Take actions when the license volume or disk usage approaches the limit.
  • Choose to obtain licenses that can manage your data volume.
  • Expand the cluster with additional reporting members to increase the disk volume. If there is a surge of reporting data generation before you upgrade your license, you may reduce the inbound volume by turning off reporting on certain Grid members or certain reporting categories.
• Do not ignore license violation warnings, such as GUI yellow banner and SNMP traps.
  • When reporting license usage approaches the limit, NIOS displays the warning messages in the yellow banner, log messages, and SNMP traps (if configured).
  • When you receive five (5) violation notifications in a rolling period of 30 days, you cannot view reports or configure report related functions. To avoid reporting interruptions, promptly address any violation notifications by contacting Infoblox Technical Support.

Note: The reporting server continues to process incoming data during the violation state. However, you cannot view any report or manage any report related functions until you fix the violation issue.

Deployment and Service Monitoring

• A reporting cluster requires that the Grid Master and reporting members have the same IPv4 or IPv6 configurations.
  • Use either IPv4 or IPv6 networks for all members. There might be an impact on the performance if you use both IPv4 and IPv6 networks. There are a few guidelines to consider before you deploy reporting clustering. For more information about the guidelines, see Guidelines for Deploying Reporting Clusters.
  • Be aware of the time lag in displaying the actual state in the reporting service status.
    • NIOS reporting monitors all communication between Splunk cluster master (on the Grid Master) and reporting members, between Grid members (forwarders) and reporting members, and among reporting members.
    • Grid Manager displays the service status to indicate any network issues. However, the status is not real-time and there might be some time lag up to 5 minutes from the moment when the issues occur or recover.
  • Regularly backup your reporting data even for a multi-site cluster deployment. Infoblox recommends that you perform reporting data backup before changing your configuration from a single indexer to a single-site cluster or multi-site cluster and from a single-site cluster to a multi-site cluster. For information, see Backing Up Reporting Data.
  • Use the Reporting Clustering Status dashboard to monitor the reporting cluster status, as described in the Reporting Clustering Dashboard.
    • If the reporting cluster is functioning properly, then the overall status is green. The status turns red if there is any network outage or reporting member goes offline, which indicates that the replication factor or search factor is not met. It might take some time for Grid Manager to change the status to green even after you fix the issue because the cluster needs to replicate buckets among peers.
  • There can be duplicated bucket data in the reporting backup FTP server.
    • In the cluster mode configuration, there is a chance of uploading multiple copies of the same bucket because reporting data backup takes data from multiple reporting members simultaneously. However, the reporting data restore process eliminates the duplicate copies of such buckets.
  • It is a good practice to backup the Infoblox Reporting and Analytics App regularly, even though the appliance backs up data from the running search head to the Grid Master periodically. By doing this, it is easier to recover the data automatically by the new search head in case of a search head failure. For information, see Backing Up and Restoring the Infoblox Reporting and Analytics App.
Other Best Practices for Deploying Reporting Clusters

- When you plan a single site or multi-site reporting cluster, make sure that you join all the relevant reporting members to the cluster immediately. Any delays in adding the reporting members might cause some data loss because peers are unable to start indexing immediately. In addition, Infoblox recommends that you validate the reporting clustering configuration before you start the reporting service, as described in Validating Reporting Clustering Configuration.

- When you need to bring down any reporting members for reasons such as maintenance and the member will be back online soon, you can use the set_reporting_cluster_maintenance_mode CLI command to suppress the cluster master to initiate any bucket fix-up activities. For more information about this command, refer to the InfobloxCLI/Guide. After completing the maintenance, use the same (set_reporting_cluster_maintenance_mode) CLI command to turn off the reporting cluster maintenance mode.

- When you upgrade from a previous release to NIOS 7.3.200 or later, the Grid will automatically be upgraded to the single indexer mode. You can change the reporting clustering configuration after the upgrade.

- When you upgrade from NIOS 7.3.200 to a later NIOS release, the Grid will retain the cluster type configured in NIOS 7.3.200.

- During a scheduled upgrade, reporting members will restart and become unavailable to receive events from other Grid members. To avoid the scenario that all reporting members might go offline about the same time, Infoblox suggests that you put reporting members in different upgrade groups and schedule different upgrade times for these upgrade groups. By doing so, there will always be some reporting members available to receive data from other Grid members. Thus, you can avoid potential data loss during scheduled upgrades.

- When you upgrade from a previous release to NIOS 7.3.200 or later, reporting data generated before you enable reporting clustering is replicated on all reporting members. Therefore, in cases when a reporting appliance is down or offline, you may experience some data loss (although this data will be captured in the reporting backup file). Infoblox recommends that you back up your reporting data before an upgrade or enabling reporting clustering.

- You cannot revert the NIOS software version after you have configured a single-site or multi-site cluster from the single indexer mode. For example, if you upgrade the Grid from NIOS 7.3.0 to NIOS 7.3.200 or later with reporting service enabled (only the single indexer mode is supported until NIOS 7.3.200), the Grid will automatically be upgraded to a single indexer mode. If you then configure a single-site or multi-site cluster after the upgrade, you cannot revert to a single indexer in the upgraded version. To configure a single indexer, you must revert the NIOS software version to NIOS 7.3.0, which may cause some data loss because not all data stored on different reporting members in the previous reporting cluster is consolidated to the single indexer.

- When you plan to move a reporting appliance from one Grid to another, you must first enable the reporting service in the new Grid and then join the reporting appliance.

- Infoblox recommends that you do not reboot the reporting appliance or restart the reporting service when performing reporting backups or restores. For information, see Backing Up Reporting Data and Restoring the Reporting Database.

- Infoblox recommends that you use appliance models with the same capacity as peers in a cluster. If you set up a reporting cluster using heterogeneous models, the appliance displays a warning message and limits the capacity of the entire cluster based on the peer that has the smallest capacity. For information about how to validate the reporting configuration, see Validating Reporting Clustering Configuration.

The following table provides example configurations for the single-site and multi-site clustering:

<table>
<thead>
<tr>
<th>Clustering Types</th>
<th>Configuration Details</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-site clustering (Replication Factor = 2)</td>
<td>Forwarder volume = 2GB per day Licensing Master: 1 X 5G Primary Site: 2 X TR-1400 (5G)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Forwarder volume: 5GB per day Licensing Master: 1 X 10G Primary Site: 2 X TR-2200</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Forwarder volume: 8GB per day Licensing Master: 2 X 10G Primary Site: 4 X TR-2200</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Forwarder volume: 8GB per day Licensing Master: 1 X 20G Primary Site: 2 X TR-4000</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Forwarder volume: 8GB per day Licensing Master: 1 X 10G Primary Site: 2 X TR-2200</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Forwarder volume: 5GB per day Licensing Master: 1 X 10G Primary Site: 4 X TR-2200</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Forwarder volume: 5GB per day Licensing Master: 1 X 10G Primary Site: 2 X TR-2200, Backup Site: 2 X TR-2200</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Forwarder volume: 5GB per day Licensing Master: 1 X 10G Primary Site: 2 X TR-2200 Backup Site: 1 X TR-2200</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Forwarder volume: 8GB per day Licensing Master: 1 X 10G Primary Site: 4 X TR-2200 Backup Site: 2 X TR-2200</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 40.4 Clustering Configuration Examples
Grid Reporting Properties

After you set up a dedicated reporting appliance in your Grid, you must configure the Grid reporting properties so you can communicate with the reporting appliance and retrieve report data through the Grid Master. In addition, you must select the correct report categories in order for the reporting server to generate the correct data in corresponding reports, as described in Configuring Grid Reporting Properties. By default, only superusers can configure the Grid reporting properties. When you enable the Grid reporting service, all members transmit data to the reporting server. You can disable data transmission from specific members to the reporting server. Before using the reporting service, you must configure the remote server to export the search results, as described in Reporting (Index) Storage Space. Once you configure the reporting server and enable the reporting service on Grid members, you can view and manage reports through the Reporting tab of Grid Manager.

Note: When you reset the appliance using the CLI command reset all or reset the database using the CLI command reset database, the reporting configurations are not preserved. If you reset the appliance, you must configure Grid reporting properties and remote server settings to use the reporting service.

Complete the following to configure the Grid reporting properties:

1. From the Administration tab -> Reporting tab, click Grid Reporting Properties from the Toolbar.
   or
   From the Grid tab, select the Grid Manager tab and click the Services tab. In the Services tab, select the Reporting tab and click Edit -> Grid Reporting Properties from the Toolbar.
2. In the Grid Reporting Properties editor, select the General -> Basic tab
3. Complete the following:
   - Reporting Server: Grid Manager displays the name of the reporting server.
   - Enable Data Indexing: Data transmission is disabled by default. You must select this check box to ensure that all Grid members transmit data to the reporting appliance. Enabling data transmissions for all members can affect the overall data consumption on the reporting server. For information about the daily maximum data consumption per day for your reporting appliance, see Table 40.5.
   - Report Category: Select the reports you want the reporting server to generate. The reporting server automatically configures data sources and configurations required to generate the reports you select here. The required data is stored in the reporting server database. By default, no report categories are selected. For a list of report categories, see Predefined Dashboards. You must select at least one reporting category for the reporting service to start working.
     - Index%: Displays the actual storage space allocated for a reporting index. You can modify this value between 0 and 100. When you enable an index category and leave it at 0%, the appliance displays an error message. Make sure that the total percentage of the index storage space for all report categories equals 100% or less than 100%. The appliance displays a warning message when the total percentage of the index storage space is less than 100%.
     - Used%: Displays the index storage space used by a reporting index.
     - IndexName: Displays the reporting index name, which are displayed on the Reporting Index Usage Statistics report.
4. Save the configuration and click Restart if it appears at the top of the screen.

Configuring Grid Reporting Properties

After you configure the reporting server, you must enable the data indexing and select at least one reporting category to ensure that the reporting service functions properly.

Note: You must select the correct report categories in order for the reporting server to generate the correct data in corresponding reports.

Complete the following to set up your reporting solution:

- Configure general reporting properties, including the selection of report categories, as described in Configuring Grid Reporting Properties.
- Specify the network port for reporting, as described in Setting the Network Port for Reporting.
- Specify email properties, as described in Configuring Email Notification Settings.
- Configure logo image for PDF delivery, as described in Configuring Logo Image in PDF Reports.

The properties you define in the Grid Reporting Properties editor apply to all the reporting members, unless you override them at specific member level. To override at the member level, see Modifying Member Reporting Properties.

Reporting (Index) Storage Space

One key configuration aspect of the reporting appliance is index space. By default, some percentage of index space is allocated on the reporting server for each report category listed in Table 40.3. For information about how to configure index space, see Configuring Grid Reporting Properties.
Each report category uses up to a certain percentage of the usable reporting hard disk space for index storage. For example, of the total 237 GB usable hard disk space of an IB-VM-800 appliance, the reporting category, **Device** uses 47.47%. For the list of default index space configured for each report category, see Table 40.5. You can modify the index percentage value between 0 and 100. When you modify this value, make sure that the total percentage for the index storage space for all categories equals exactly 100%. You can set the index percentage to a value less than 100% to reserve certain percentage for future use. If the total percentage of the index space usage exceeds 100%, the appliance displays an error message. Note that the reporting appliance removes the oldest data when you reduce the index space percentage for a category to a value that is lower than the used percentage by the existing data. For information about the maximum index size and number of days the reporting data is retained, see Table 40.8. Also, ensure that its host name has only alphanumeric characters, underscores, dots, and dashes.

**Note:** For usable reporting hard disk space for each appliance model, see Table 40.2.

### Table 40.5 Default Index Space Configured for Each Report Category

<table>
<thead>
<tr>
<th>Report Category</th>
<th>Default Index Space (%) Adjustable by User</th>
<th>Total Reporting Disk Space Used for Index Storage (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Log</td>
<td>0%</td>
<td>Usable reporting hard disk space x 20%</td>
</tr>
<tr>
<td>DNS Query</td>
<td>20%</td>
<td>Usable reporting hard disk space x 20%</td>
</tr>
<tr>
<td>DNS Performance</td>
<td>20%</td>
<td>Usable reporting hard disk space x 20%</td>
</tr>
<tr>
<td>DNS Record Scavenging</td>
<td>39%</td>
<td>Usable reporting hard disk space x 39%</td>
</tr>
<tr>
<td>DNS Query Capture</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>DHCP Performance</td>
<td>20%</td>
<td>Usable reporting hard disk space x 20%</td>
</tr>
<tr>
<td>DHCP Fingerprint</td>
<td>5%</td>
<td>Usable reporting hard disk space x 5%</td>
</tr>
<tr>
<td>DHCP Lease History</td>
<td>1%</td>
<td>Usable reporting hard disk space x 1%</td>
</tr>
<tr>
<td>DDI Utilization</td>
<td>0%</td>
<td>Usable reporting hard disk space is broken down between ib_dtc and ib_dtc_summary internally.</td>
</tr>
<tr>
<td>Security Network User</td>
<td>15%</td>
<td>Usable reporting hard disk space x 15%</td>
</tr>
<tr>
<td>DNS Traffic Control</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>Cloud</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>System Utilization</td>
<td>15%</td>
<td>Usable reporting hard disk space x 15%</td>
</tr>
<tr>
<td>Device</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>Ecosystem Subscription</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>Ecosystem Publication</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>License</td>
<td>0%</td>
<td></td>
</tr>
</tbody>
</table>

### Modifying Member Reporting Properties

To modify reporting properties for a reporting member:

1. From the **Grid** tab -> **Grid Manager** tab -> **Services** tab, select the **Reporting** service and click the **Grid_member** check box, and then click the **Edit** icon.
2. In the **Reporting Member Properties** editor, select the **General** tab and click **Override**.
3. Under **Reporting Settings**, complete the following:
   - **Enable data forwarding to the indexer on this member**: Select this check box to enable data transmissions to the reporting server. If you do not select this check box, a member will not forward data to the indexer and reporting service is disabled on that member.
   - **Select the data categories to forward**: Select the report categories for which you want this member to forward data to the reporting server. Clear the report categories for which you do not want this member to forward data to the reporting server.

**Note:** The member configured as an indexer displays only the **Audit Log** category.

4. Save the configuration.
Defining Interface for Reporting Traffic

On a Grid member, you can define the network interface you want the member to use for sending reporting data to the reporting server. To define network interface on the Grid member for reporting traffic, complete the following:

1. From the Grid tab -> Grid Manager tab -> Services tab, select the Reporting service and click the Grid_member check box, and then click the Edit icon.
2. In the Reporting Member Properties editor, select the General -> Advanced tab, and then complete the following:
   - Forwarding interface used for reporting traffic: From the drop-down list, select the interface that you want this member to use to send reporting data. Note that you must properly configure the interfaces on the member for them to appear in the drop-down list.
   - After a NIOS upgrade to version 8.1.x or later, if you had selected Any from the drop-down list, the LAN1 (or VIP for HA configurations) subnet is used as the static route. Select MGMT if you want to continue using the management port for grid communication. Selecting MGMT enables the MGMT subnet to be used as the static route.
   - Statistics Collection Top Grid_member (minutes): Enter the time in HH:MM:SS AM/PM format. You can also click the Clock icon to select a time from the drop-down list.

3. Save the configuration.

Setting the Network Port for Reporting

All Grid members use port 9997 for reporting service by default. This port is used for data transmissions between the reporting member and other members. Ensure that you configure your firewall rules to allow traffic on this port. You can designate another network port for reporting purposes. To set the network port for reporting:

1. From the Administration tab, select the Reporting tab -> expand the Toolbar and click Grid Reporting Properties. or
2. From the Grid tab -> Grid Manager tab -> Services tab, select the Reporting service and click the Grid_member check box, and then click Edit -> Grid Reporting Properties from the Toolbar.
3. In the Grid Reporting Properties editor, select the General -> Advanced tab and complete the following:
   - Port: Enter the port number you want to use for reporting purposes. The default port is 9997.
   - Interface: Enter the interface you want to use for sending data to the reporting server.

4. Save the configuration.

Specifying the Data Generation Interval for Reports

You can specify the time interval when the appliance generates data for the DNS Statistics per View and DNS Statistics per Zone reports. The default value for the data generation interval for these reports is one day (86400 seconds). You can specify different data generation intervals for the DNS Statistics per View and DNS Statistics per Zone reports.

To specify the data generation interval for DNS Statistics per View and DNS Statistics per Zone reports:

1. From the Administration tab, select the Reporting tab -> expand the Toolbar and click Grid Reporting Properties. or
   - From the Grid tab -> Grid Manager tab and click the Services tab. In the Services tab, select the Reporting tab and click Edit -> Grid Reporting Properties from the Toolbar.
2. In the Grid Reporting Properties editor, select the Data Generation Schedule tab and complete the following:
   - Data Generation: Enter the time in HH:MM:SS AM/PM format. You can also click the Clock icon to select a time from the drop-down list.
   - Interval: Enter the interval in minutes. You can also click the Clock icon to select an interval from the drop-down list.

3. Save the configuration.

For more information about the reports, see DNS Statistics per DNS View and DNS Statistics per Zone

Configuring Threat Protection Data

You can use this feature only if the Threat Protection and Threat Protection Update licenses are installed on the Infoblox Advanced Appliance. When you configure this feature, you receive threat protection events in the syslog. The events logged include threat protection rules and the source IPs that triggered the rules. For information about how to monitor these events using the syslog, see Monitoring through Syslog.

For certain threat protection reports, accumulated statistics for each unique IP/rule pair are collected. You can control the volume of data collected per member using the following options:

- Top IP/Rule Statistics Collection Limit: This option limits the collection of accumulated statistics to the top N unique IP/rule pairs.
- IP/RuleStatisticsCollectionInterval(minutes): The interval at which the accumulated statistics for the top N unique IP/rule pairs are collected. The smaller the interval, the finer the granularity of the accumulated statistics in terms of time, but the data volume will be higher.

Based on your configuration, the reporting appliance displays data in the following threat protection reports:

- Threat Protection Top Rules Logged
- Threat Protection Top Rules Logged by Source

Copyright ©2019, Infoblox, Inc. All right reserved.
**Note:** When threat details are missing for a non-local RPZ feed zone entries, it is recommended to check if the associated feed zone’s TSIG key is configured.

**Note:** To enable threat protection reports, you must select the Security report category in the Grid Reporting Properties editor. To select the Security check box, go to the Reporting tab -> Grid Reporting Properties -> General tab -> Basic tab -> select the Security check box under Report Category. Ensure that you set the Security Index% to an optimal level so the reporting database has enough storage space to accommodate all reporting data. For information about how to configure the index %, see Configuring Grid Reporting Properties.

To configure the data collection limit:

1. From the Administration tab, select the Reporting tab and click Grid Reporting Properties from the Toolbar.
   or From the Grid tab, select the Grid Manager tab and click the Services tab. In the Services tab, select the Reporting tab and click Edit -> Grid Reporting Properties from the Toolbar.
2. In the Grid Reporting Properties editor, select the Threat Protection tab and complete the following:
   - **Top IP/Rule Statistics Collection Limit:** Enter the maximum number of the top N unique source IP/rule pairs for data collection. For example, if you specify 20, the appliance collects data for the top 20 unique source IP/rule pairs.
   - **IP/Rule Statistics Collection Interval (minutes):** Enter the time interval at which the reporting appliance updates data. For example, if you specify the interval as 60 minutes, the appliance updates data at a 60 minute interval.
3. Click Save & Close.

**Monitoring DNS Client Queries**

You can view the presence of clients in the network that are sending large numbers of queries to DNS zones or DNS domains. To monitor the top clients querying DNS zones, do the following:

1. From the Administration tab, select the Reporting tab -> expand the Toolbar and click Grid Reporting Properties.
   or From the Grid tab, select the Grid Manager tab and click the Services tab. In the Services tab, select the Reporting tab and click Edit -> Grid Reporting Properties from the Toolbar.
2. In the Grid Reporting Properties editor, select the Basic tab -> DNS.
3. Under DNS Top Clients Per Domain, select the Monitor Queries made to the following zones check box. Only authoritative zones are supported, to a limit of 1000 zones for monitoring purposes.
   - To select zones one at a time, choose individual check boxes. Click the Add icon and select Add Domain or Bulk Add Domains to add new zone information for excluding.
   - To specify the number of clients to be listed, choose the Top N Limit value. The default value is 10.

**Monitoring IP Block Group Queries**

You can view the user defined IP block groups that are querying DNS domains. To monitor the IP Block Groups, do the following:

1. From the Administration tab, select the Reporting tab -> expand the Toolbar and click Grid Reporting Properties.
   or From the Grid tab, select the Grid Manager tab and click the Services tab. In the Services tab, select the Reporting tab and click Edit -> Grid Reporting Properties from the Toolbar.
2. In the Grid Reporting Properties editor, select the Basic tab -> DNS.
3. Under DNS Query trend per IP Block, select the Monitor Queries made from the following groups check box.
   - Click the Add icon to add a group to the group table. From the drop-down list, click Select Group to select groups in the Group Selector dialog box, or click Bulk Add Groups to add multiple groups.
   - To select all groups, select the Group check box. Or, select individual check box to select the group one at a time.
   - To delete a group, select the group and click the Delete icon.

**Configuring DNS RPZ Rule Hits**

You can specify a limit to display the number of top clients, who receive re-written responses through the RPZ, in DNS Top RPZ Hits. You can also specify the total number of RPZ entries for each client.

1. From the Administration tab, select the Reporting tab -> expand the Toolbar and click Grid Reporting Properties.
   or From the Grid tab, select the Grid Manager tab and click the Services tab. In the Services tab, select the Reporting tab and click Edit -> Grid Reporting Properties from the Toolbar.
2. In the Grid Reporting Properties editor, select the Basic tab -> DNS.
3. Under DNS RPZ Rule Hit Configuration, complete the following:
   - Enter a value for Top N Limit to specify the maximum number of top clients that can be listed in the report.
   - Specify the Total RPZ Entries per Client. This indicates the number of entries for each client in RPZ.

**Note:** You have to select the Security check box before you define values here. To select the check box, Reporting tab -> Grid Reporting Properties -> General tab -> Basic tab -> select the check box Security under Report Category.

---

Copyright ©2019, Infoblox, Inc. All rights reserved.
Forwarding Syslog Data to the Reporting Server

You can control the kind of syslog data forwarded to the indexer from the Grid members. You can search for syslog events (search string) in the Reporting tab -> Search tab. The syslog events you see in the Search tab depends on the syslog categories that you specify in both the Grid Reporting and Member Reporting Properties. The Search tab displays syslog events for the selected syslog categories at both the Grid Reporting Properties and Member Reporting Properties. For information, see About Searches.

To specify syslog data categories:

1. From the Administration tab, select the Reporting tab -> expand the Toolbar and click Grid Reporting Properties. 
or
   Member: From the Grid tab, select the Grid Manager tab and click the Services tab. In the Services tab, select the Reporting tab -> m ember check box and then click the Edit icon.
2. In the Grid Reporting Properties or Reporting Member Properties editor, select the Syslog Data tab and complete the following:
   Click Override in the Reporting Member Properties editor to override the settings configured at the Grid reporting level. To inherit the same properties as the Grid, click Inherit.
   - **Source:** From the drop-down list, select which syslog messages the appliance sends to the external syslog server:
     - Any: The appliance sends both internal and external syslog messages.
     - Internal: The appliance sends syslog messages that it generates.
     - External: The appliance sends syslog messages that it receives from other devices, such as syslog servers and routers.
   - **Severity:** Choose a severity filter from the drop-down list. When you choose a severity level, the appliance sends log messages with the selected levels and the levels above it. The severity levels range from the lowest, debug, to the highest, emerg. For example, if you choose debug, the appliance sends all syslog messages to the server. If you choose err, the appliance sends messages with severity levels err, crit, alert, and emerg.
     - **Send selected categories:** Select this to configure logging categories from the list of available logging categories. Use the arrows to move logging categories from the Available table to the Selected table and vice versa. The appliance sends syslog messages for the categories that are in the Selected table. When you select this option, you must add at least one logging category.
     - The syslog messages are prefixed with a category name to which it belongs. Also, the RPZ events logged in the syslog messages uses specific prefixes for the selected categories. Note that the syslog messages are prefixed when you set logging categories for at least one external syslog server, even if you set other external syslog servers as Send All.

3. Save the configuration and click Restart if it appears at the top of the screen.

About IP Blocks and IP Block Groups

You can configure IP addresses, subnets, or a mix of multiple IP addresses and subnets into IP blocks, and then assign them to IP block groups for monitoring and tracking queries made to specific IP blocks. For information about adding IP addresses, see Adding IP Blocks. You can also configure as many groups as necessary and assign them to specific clients. Note that assigning more IP block groups results in monitoring more queries, which may affect the performance of the reporting server. You can generate a report to monitor queries made to these user-defined IP block groups or IP blocks. For information, see DNS Query Trend per IP Block Group.

Guidelines while configuring IP blocks:

- You cannot configure arbitrary IP address ranges, such as 192.168.0.1 to 192.168.0.100 as an IP block.
- You cannot add or modify an IP block that overlaps with another IP block in a different group. However, you can add an IP block that overlaps with another IP block in the same IP block group.

Note: The appliance restarts the DNS service after you assign or unassign an IP block group at the Grid or member level. Also, the appliance restarts the DNS service when you modify or delete an IP address or IP block group assigned to the Grid or member or when you add, modify, or delete an IP block in such IP block groups.
You can do the following in the Groups panel:

- Add IP block groups, as described in Adding IP Block Groups.
- Modify IP block groups, as described in Modifying IP Block Groups.
- Add IP block, as described in Adding IP Blocks.
- Modify IP blocks, as described in Modifying IP Blocks.
- Delete IP block groups and IP blocks, as described in Deleting IP Block Groups and IP Blocks.
- Print IP block groups and IP blocks, as described in Printing IP Block Groups and IP Blocks.
- Export IP block groups and IP blocks, as described in Exporting IP Block Groups and IP Blocks.

In addition, you can also do the following:

- Use filters or the Go to function to navigate to a specific group. You can also create quick filters to save frequently used filter criteria. For information about how to use quick filters, see Using Quick Filters.
- Use Global Search to search for IP block groups and IP blocks. For information, see Global Search.
- Use Smart Folders to organize IP block groups and IP blocks. For information, see About Smart Folders.
- Import and export groups in CSV format. For more information about CSV import feature, see About CSV Import.

Adding IP Block Groups

To add a new group:

1. From the Administration tab, select the Reporting tab -> Group -> Add.
   or
   From the Administration tab, select the Reporting tab, expand the Toolbar and click Add -> IP Block Group.
2. In the Add IP Block Group wizard, complete the following:
   - Name: Enter the name of the group.
   - Comment: Enter useful information about the group.
3. Do one of the following:
   - Click Save & Close to add the IP block group and close the wizard.
   - Click Save & Edit to add the IP block group and launch the editor. You can edit the details.
   - Click Save & New to add the IP block group and launch the wizard again to add another group.
   - Click Save & Open to add the IP block group and open the IP block group.

Modifying IP Block Groups

1. From the Administration tab, select the Reporting tab -> Group -> Edit.
2. In the General tab of the IP Block Group editor, you can modify the group name and comment.
3. Click Save & Close to save the configuration.

Note: You can perform inline editing by double-clicking the row of data that you want to modify. The appliance displays the inline editing editor in the selected row. Click Save after modifying the data.

Adding IP Blocks

In a group, you can add as many subnets/IP addresses as necessary. Note that adding more IP addresses results in monitoring more queries, which may affect the performance of the reporting server.

1. From the Administration tab, select the Reporting tab -> Group -> Add.
   or
   From the Administration tab, select the Reporting tab, expand the Toolbar and click Add -> IP Block.
2. In the Add IP Block wizard, complete the following:
   - Group: Click Select to select a group. When there are multiple groups, Grid Manager displays the Group Selector dialog box to select a group. Click a group name in the dialog box. You can use filters or the Go to function to narrow down the list.
   - Address: Enter the source IPv4/IPv6 addresses or the IPv4/IPv6 subnets.
   - Comment: Enter useful information about the IP block.
3. Do one of the following:
   - Click Save & Edit to add an IP address or IP block and launch the editor. You can edit the details.
   - Click Save & New to add an IP address or IP block and launch the wizard again to add another IP block.
   - Click Save & Close to add an IP address or IP block and close the wizard.

Modifying IP Blocks

1. From the Administration tab, select the Reporting tab -> Group.
2. Select an IP address or IP block you want to modify and click the Edit icon.
3. In the General tab of the IP Block editor, modify the IP address or comment.
4. Click Save to save the configuration.

**Note:** You can modify description by using inline editing. Double-click the row that you want to modify, the appliance displays the inline editing editor in the selected row. Click Save after modifying comment. You cannot modify IP address using inline editing editor.

### Deleting IP Block Groups and IP Blocks

1. For IP block groups: From the Administration tab, select the Reporting tab -> Group.
2. For IP blocks: From the Administration tab, select the Reporting tab -> Group -> IP block.
3. Click the Delete icon.
4. In the Delete Confirmation dialog box, click Yes.

### Exporting IP Block Groups and IP Blocks

You can export displayed data or you can export the group list in CSV (comma separated value) format. Exporting group lists or group data may take a few moments based on the amount of exported data.

**To export displayed data:**

1. For IP block groups: From the Administration tab, select the Reporting tab -> Group.
2. For IP blocks: From the Administration tab, select the Reporting tab -> Group -> IP block.
3. From the Export drop-down menu, select Export visible data. For more information on how to export, see Exporting Displayed Data.

**To export all data to a CSV file:**

1. For IP block groups: From the Administration tab, select the Reporting tab -> Group.
2. For IP blocks: From the Administration tab, select the Reporting tab -> Group -> IP block.
3. From the Export drop-down menu, select Export data in Infoblox CSV Import format. For more information on how to export, see Exporting Data to Files.

### Printing IP Block Groups and IP Blocks

1. For IP block groups: From the Administration tab, select the Reporting tab -> Group. For IP blocks: From the Administration tab, select the Reporting tab -> Group -> IP block.
2. Click the Print icon. For more information on how to print, see Printing from Grid Manager.

### Reporting User Interface Overview

When you access the Reporting tab in Grid Manager, you can do the following:

- View and analyze all of your DNS, DHCP, and IPAM data.
- View the reporting data in the form of charts and tables.
- Use the Search tab to create or edit searches.

The key options in the Reporting tab are: Home Dashboards, Dashboards, Reports, Alerts, Search, Pivot, Administration, and Reporting Help. For more information about these options, see Table 40.6. Figure 40.8 Reporting Tab Overview
The following table summarizes the different tabs and key options that are available in the Reporting tab:

<table>
<thead>
<tr>
<th>Tab Name</th>
<th>Purpose</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>Email notification settings Server Logging</td>
<td>For information, see <a href="#">Configuring Email Notification Settings</a></td>
</tr>
<tr>
<td>Home Dashboard</td>
<td>Overall summary view for the reporting data in your Grid</td>
<td>For information, see <a href="#">Home Dashboards</a></td>
</tr>
<tr>
<td>Dashboard</td>
<td>Provide table and graph views for the reporting data in your Grid.</td>
<td>For information, see <a href="#">Home Dashboards</a></td>
</tr>
<tr>
<td>Reports</td>
<td>Saved searches that retrieve specific type of reporting data</td>
<td>For information, see <a href="#">About Reports</a></td>
</tr>
<tr>
<td>Alerts</td>
<td>Set alerts to trigger actions when certain events occur</td>
<td>For information, see <a href="#">About Alerts</a></td>
</tr>
<tr>
<td>Search</td>
<td>Create a search interactively from scratch and save it as a dashboard panel, alert and report.</td>
<td>For information, see <a href="#">About Searches</a></td>
</tr>
<tr>
<td>Pivot</td>
<td>Refer to Splunk documentation for more information.</td>
<td></td>
</tr>
<tr>
<td>Administration</td>
<td>• Set up</td>
<td>For information, see <a href="#">Reporting (Index) Storage Space</a></td>
</tr>
<tr>
<td></td>
<td>• Permissions</td>
<td>For information, see <a href="#">Administrative Permissions</a></td>
</tr>
<tr>
<td>Reporting Help</td>
<td>Quick help on some of the reporting topics.</td>
<td></td>
</tr>
</tbody>
</table>

Hierarchy settings for all the navigation menu options (listed in the Table 40.6) are available in the default.xml file.

**WARNING:** Infoblox recommends that you do not modify the default.xml file. The navigation menu is built on a custom XML structure that is stored as default.xml in the navigation directory (from the Reporting tab, select the Settings tab -> User Interface -> Navigation Menus -> default). Editing this file changes the specific default settings for the reporting features and your changes become permanent. In addition, you might not be able to see the latest changes made by Infoblox. To restore the default settings, you must reset the NIOS appliance to its original factory settings. For information, see [Resetting a NIOS Appliance to Factory Settings](#).
**Home Dashboards**

You can view the overall summary of DNS, DHCP, and IPAM activities in the **Home Dashboard** page. This page presents a summary view of the following:

- **DDI Summary**: Presents statistical information about the DNS, DHCP, and IPAM activities of all Grid members.
- **DNS**: Displays the statistical summary of DNS activities. You can export the search results, open in search, and refresh.
- **DHCP**: Displays the statistical summary of DHCP activities. You can export the search results, open in search, and refresh.
- **IPAM**: Displays the summary of the **Top10/IPAMv4UtilizedNetworks** dashboard.
- **Reporting Health**: You can view the license usage by the reporting server:
  - **Today’s License Usage**: Current license usage by the indexer.
  - **License Usage Trend per Member**: License usage by the indexer per member.

![Figure 40.9 Reporting Home Dashboard](image)

**About Searches**

Searches are criteria that the reporting server uses to save reports and dashboard panels. Each predefined report has an associated search. For more information, refer to the official Splunk documentation: [http://docs.splunk.com/Documentation](http://docs.splunk.com/Documentation).

To run a search:

1. From the **Reporting** tab, select the **Search** tab.
2. Enter the search criteria and then click the Search icon.

The search results are displayed in the **New Search** panel, as illustrated in the **New Search View**. In the **New Search** panel, you can save search results as **Reports**, **Dashboard Panel**, and **Alerts**. When you deploy reporting clustering, we enable Splunk configuration to prevent data loss from forwarders, which may cause duplicated events in the indexer under certain circumstances. When you view reports and dashboards, the events that are already deduped are not duplicated again. However, if you view raw search events (such as write your own search against the indexed data directly), you may still see the duplicated events.

The search results are based on the most seen events for the dashboards listed in **Table 40.7**. To know more about dedup searches, reports, or dashboards, refer to [http://docs.splunk.com/Documentation/Splunk/6.3.3/SearchReference/Dedup](http://docs.splunk.com/Documentation/Splunk/6.3.3/SearchReference/Dedup).

**Note**: When you click **Open in Search**, the content of the entire page (alert/dashboard/report) is encoded and displayed in the **Search** page. To avoid encoding, go to **Activity** -> **Jobs**. The **Jobs** page lists the search job history in the form of links. The top one is the latest search job executed by the alert or dashboard or report. The search string is not encoded when you click this link to run the search.

**Table 40.7 Dashboards and Deduplicate Key(s)**

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Deduplicate Key(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactive IP Addresses</td>
<td>Network view + IP address</td>
</tr>
</tbody>
</table>

Copyright ©2019, Infoblox, Inc. All right reserved.
Best Practices for Customizing Searches
You can optimize the performance of your reporting server and more efficiently view and manage your reports. Depending on the type of search and the data you want to search for, Infoblox recommends that you use the following guidelines:

- Specify shorter start and end times whenever possible.
- Time range is one of the most important factor for search performance. Depending on the number of events that need to be loaded from the disk, it might take a long time when you specify a wider time range as it involves a large amount of data.
- Be specific about the fields you use.
  - Rare searches are faster than dense searches, so be specific whenever possible.
  - Start a search from a smaller dataset and then gradually apply it to bigger dataset.
  - When experimenting searches, start with a small date and time range, and then apply it to a bigger time range only when it is optimized.
- If a search is running for a long time, you can use the Pause and Stop buttons.
- You can tune the search criteria and run it again if you stop an ongoing search jobs.
- Configure the panels to display data only if you have specific input instead of adding too many panels to the dashboard.
- Scheduling expensive searches.
  - You can configure reports and dashboards by scheduling searches because prefetched search results are displayed each time the reports and dashboards are opened. This reduces the workload on the reporting server without data freshness.
- Stagger scheduled searches.

Try to stagger your searches whenever possible. When you define how often the reporting server runs a search, be aware of other searches that the server is running. When you schedule the server to run many searches at the same time, the server performance can be negatively affected.

Creating Reports from a Search

You can create reports by saving a search as a report. To save a search as a report:

1. From the Reporting tab, select the Search tab.
2. Enter the search criteria and then click the Search icon. The search results are displayed in the New Search panel.
3. From the Save As drop-down list, click Report to generate a report.
4. Enter title and description.
5. Click Save.
6. Do one of the following in the Your report has been created dialog box:
   - Click View to view your report on the Report page.
   - Click Continue Editing to edit.
   - Click Add to Dashboard to add new report to the dashboard panel.

You can also complete the following settings in the Your report has been created dialog box:

- Permissions: Click this to edit permissions for your report, as described in Editing Permissions.
- Schedule: Click this to schedule a report. For information about scheduling reports, see Scheduling Reports.
- Acceleration: For more information, refer to the Splunk documentation.

Saving a Search as a Dashboard Panel

You can save a search as a dashboard panel.
Do the following to save a search as a dashboard panel:

1. From the Reporting tab, select the Search tab.
2. Enter the search criteria and then click the Search icon. The search results are displayed in the New Search panel.
3. From the Save As drop-down list, click Dashboard Panel to create a dashboard panel.
4. Click View Dashboard to view dashboard in the Dashboard panel. For information, see Home Dashboards.

Exporting Search Results

You can export the data in the selected search in CSV (comma separated value) or XML format. Note that this may take a long time depending on the amount of data you want to export. To schedule the export of search results to an FTP or SCP or TFTP server configured in the Setup page, select File Transfer Action when creating a scheduled alert, as described in Creating Scheduled Alerts.
To export data in a selected search:

1. From the Reporting tab, select the Search tab.
2. Enter the search criteria and then click the Search icon. The search results are displayed in the New Search panel.
3. Click the Export icon to export search results.
4. In the Export Results dialog box, complete the following:
   - Format: Select CSV or XML from the Format drop-down list.
   - File Name: Specify a file name for the export file. This is optional.
   - Number of Results: (Limited or Unlimited). If you select Limited, enter the number of results to be exported in the Max Result
Saving Search as Alerts

To save a search as an alert:

1. From the Reporting tab, select the Search tab.
2. Enter the search criteria and then click the Search icon.
3. From the Save As drop-down list, click Alert.
4. In the Save As Alert dialog box, specify all alert settings. For information about scheduling alerts, see Creating Scheduled Alerts.
5. Click Save.

About Alerts

You can configure alerts to trigger actions when certain events occur. When you set up an alert, search results trigger an alert action if they match the alert conditions. You can configure an alert to send an email notification, SNMP trap, and log a message in the syslog. Note that alerts are executed based on update frequencies for each corresponding search. For example, DHCP Lease History alerts are executed every 10 minutes, and Device Trend alerts are executed every 30 minutes at the 17th and 47th minutes of each hour (one minute after the search updates). For information about search indexes and update time intervals, see Reporting Indexes and Update Time Intervals. You can also throttle an alert if you want to change its frequency. For more information, refer to the Splunk documentation.

You can do the following in the Alerts page:

- Create scheduled alerts, as described in Creating Scheduled Alerts.
- Edit permissions, as described in Editing Permissions.
- Edit alert type, trigger condition, and alert actions, as described in Editing Alerts.
- Clone an alert, as described in Cloning Alerts.

Creating Scheduled Alerts

You can schedule an alert to notify when a scheduled report returns results that meet a specific condition. The appliances sends an alert when it encounters the trigger condition.

1. From the Reporting tab, select the Alerts tab -> select an alert and click Open in Search.
2. From the Save As drop-down list, click Alert.
3. In the Save As Alert dialog box, complete the following:
   - Specify the title and description.
   - Alert Type: Select Scheduled
   - Time Range: Specify the time range. For example you can select Run Every Day.
   - Schedule At: Specify the time.
   - Trigger Condition: Specify trigger conditions. For more information, refer to the Splunk documentation.
   - Trigger Actions: Click this to configure alert actions. You can select the following:
     - Send SNMP Trap: Select this to enable SNMP traps. For information about how to trigger SNMP traps for reporting event types, see Defining Thresholds for Traps.
     - Send email: Select this to send alert notification through email. You can specify email address in the To text box.
     - Send to Syslog: Select this to log a message in the syslog. If you configure this option with an alert, the message goes to the syslog on the reporting member or indexer.
     - File Transfer Action: Select this to upload the search results to an FTP or SCP or TFTP server configured in the Set up page. For information, see Reporting (Index) Storage Space.
4. Click Save.

Editing Alerts

You can edit alert type, trigger condition, and alert actions, as follows:

1. From the Reporting tab, select the Alerts tab -> select an alert.
2. From the Edit drop-down list, select Edit Alert Type and Trigger Condition to edit alert settings. In the Edit Alert Type and Trigger Condition dialog box, make the required changes. For information, see Creating Scheduled Alerts.
   or
   From the Edit drop-down list, select Edit Actions to edit alert actions. In the Edit Actions dialog box, make the required changes. For information, see Creating Scheduled Alerts.
3. Click Save.

Cloning Alerts
1. From the Reporting tab, select the Alerts tab.
2. Select an alert you want to clone, click Edit -> Clone.
3. Enter a new title, ID, and description. Click Clone Alert.
4. Optionally, you can click Open in Search to open the cloned alert in the Search page.
5. Click View, and do one of the following in the You report has been created dialog box:
   - Click View to view your report on the Report page.
   - Click Continue Editing to edit.
   - Click Add to Dashboard to add new report to the dashboard panel.

You can also complete the following settings in the You report has been created dialog box:

- Permissions: Click this to edit permissions for your report, as described in Editing Permissions.
- Schedule: Click this to schedule a report, as described in Scheduling Reports.
- Acceleration: For information, refer to the Splunk documentation.

### Configuring Email Notification Settings

You can enable the appliance to send email messages to specified recipients when the alert is triggered. You can configure email settings for alerts, scheduled reports, and scheduled PDF delivery.

To configure email properties for alerts and PDF delivery:

1. From the Reporting tab -> Settings tab -> click Server settings.
2. Click Email settings.
3. Specify the mail host. The default is local host.
4. Optionally, you can specify user name and password.
5. Specify Email Format.
6. In the Specify PDF Report Settings, specify the paper size, paper orientation, and also the path to logo image.
7. Click Save.

**Note:** You can configure email addresses when scheduling dashboard PDFs, scheduling reports, and creating alerts.

### About Reports

Infoblox provides reports that are named by core network service functions, such as DNS query and system utilization. Reports contain predefined search criteria that retrieve specific data from the reporting database. Each report is associated with a search. It is not recommended to modify predefined reports. However, when you run a search, you can save it as reports and share it with other users. You can also create a new report by cloning an existing report, and then modify the search criteria.

You can also create a personal report in two different ways:

- Clone a report, as described in Cloning Reports.
- Saving a search as a report, as described in Creating Reports from a Search.

**Note:** IDNs are not supported on the reporting server. The reporting server manages IDNs in punycode. The reports generated by collecting reporting data from the DNS server displays all the data in punycode only.

When you upgrade to 7.3.x, all NIOS Global reports are migrated to the Dashboards panel without filters. However, the filter conditions configured in NIOS are reflected in the Dashboards panel. All NIOS System and Global searches are migrated to the Reports panel.

You can do the following in the Reports tab:

1. From the Reporting tab, select the Reports tab -> select a report.
2. In the Reports panel, you can do the following:
   - Open a report in the Search page and edit the report using the Save As menu. For information, see About Searches.
   - You can do the following using the Edit drop-down list:
     - Edit Description
     - Edit Permissions, as described in Editing Permissions.
     - Edit Schedule, as described in Scheduling Reports.
     - Clone a report, as described in Cloning Reports.

### Reporting Indexes and Update Time Intervals

Table 40.8 lists the search indexes that the reporting server uses to generate reports. It contains information about the frequency of the summary report updates for each report and the percentage of the total index space allocated for each report category. Use this information to plan your reporting strategy for the Grid so you can optimize the performance of the reporting server.

Each summary report or search has its own update frequency. For example, the DNS Top Requested Domain report updates its data every 30 minutes, starting at the 4th minute of each half hour. It collects report data during the first 30 minutes of the previous 60 minutes. For example, if the report starts an update at 6:04 a.m., the data it collects is from 5:04 a.m. to 5:34 a.m.

The reporting server also uses this information to generate alerts. For example, once configured, Top Devices Identified alerts are executed at the...
17th and 47th minutes of each hour (one minute after each update), regardless of whether DHCP fingerprint detection is enabled or disabled. For information about alerts, see About Alerts.

Note: The maximum retention period for the reporting data is 136 years. However, the data is removed from the database if the data exceeds the maximum limit for a reporting index and when the data crosses the retention period (after 136 years).

Table 40.8 Reporting Indexes

<table>
<thead>
<tr>
<th>Indexes</th>
<th>Reports/ Searches</th>
<th>Summary Report Data Updates</th>
<th>Default Max Index Store</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device (Discovery)</td>
<td></td>
<td></td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td>Inactive IP Addresses</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Capacity Utilization by Device</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Capacity Trend</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Capacity Delta by Device</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>End Host History</td>
<td>N/A</td>
<td>0%</td>
</tr>
<tr>
<td>IPAMv4</td>
<td>IPAMv4 Network Usage Statistics (Detailed)</td>
<td>N/A</td>
<td>5%</td>
</tr>
<tr>
<td></td>
<td>DNS Statistics per DNS View (Detailed)</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Statistics per Zone (Detailed)</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPAMv4 Top Utilized Networks (Detailed)</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Object Count Trend for Flex Grid License</td>
<td>N/A, Data is generated once every 24 hours</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>DDNS Update Rate Trend</td>
<td>N/A</td>
<td>10%</td>
</tr>
<tr>
<td></td>
<td>DNS Response Latency Trend (Summary)</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Cache Hit Rate Trend</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Query Rate by Query Type</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Query Rate by Server (Detailed)</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Replies Trend</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Query Trend Per IP Block Group</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FireEye Alerts</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>DNS Summary</td>
<td>DDNS Update Rate Trend (Summary)</td>
<td>Every 30 minutes, starting at the 6th minute of each half hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td>10%</td>
</tr>
<tr>
<td></td>
<td>DNS Response Latency Trend (Summary)</td>
<td>Every 30 minutes, starting at the 20th minute of each half hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Top Requested Domain Names (Summary)</td>
<td>Every 30 minutes, starting at the 4th minute of each half hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Cache Hit Rate Trend (Summary)</td>
<td>Every 30 minutes, starting at the 8th minute of each half hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Effective Peak Usage Trend for Flex Grid License</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Top Clients (Summary)</td>
<td>Every 30 minutes, starting at the 2nd minute of each half hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Query Rate by Query Type (Summary)</td>
<td>Every 30 minutes, starting at the 10th minute of each half hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Query Rate by Member (Summary)</td>
<td>Every 30 minutes, starting at the 12th minute of each half hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Frequency</td>
<td>Time Frame</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------</td>
<td>------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>DNS Daily Query Rate by Member</td>
<td>Every day, starting at 00:32 each day. Data covers from 00:00 of yesterday to 00:00 of today.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Daily Peak Hour Query Rate by Member</td>
<td>Every 60 minutes, starting at the 34th minute of each hour. Data covers from the top of last hour to the top of current hour.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Replies Trend</td>
<td>Every 30 minutes, starting at the 18th minute of each hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top Clients Per Domain</td>
<td>Every 30 minutes, starting at the 3rd minute of each hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top NXDOMAIN / NOERROR (no data)</td>
<td>Every 30 minutes, starting at the 5th minute of each hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top SERVFAIL Errors Sent</td>
<td>Every 30 minutes, starting at the 6th minute of each hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top SERVFAIL Errors Received</td>
<td>Every 30 minutes, starting at the 7th minute of each hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top Timed-Out Recursive Queries</td>
<td>Every 30 minutes, starting at the 8th minute of each hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top RPZ Hits</td>
<td>Every 10 minutes, starting at the 2nd minute of each 10 minute. Data covers from 20 minute ago to 10 minute ago.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top RPZ Hits by Clients</td>
<td>Every 10 minutes, starting at the 2nd minute of each 10 minute. Data covers from 20 minute ago to 10 minute ago.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Scavenged Object Count Trend</td>
<td>Every 30 minutes, starting at every 21th and 51st minute of each hour.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCPv4 Usage Statistics</td>
<td>N/A</td>
<td>2 Months</td>
<td></td>
</tr>
<tr>
<td>DHCPv4 Range Utilization Trend</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Message Rate Trend</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Top Lease Clients</td>
<td>Every 30 minutes, starting at the 16th minute of each hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCPv4 Range Utilization Trend</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCPv4 Usage Trend</td>
<td>Every 8 hours, starting at the 24th minute of each hour. Data covers the first 8 hours of the previous 8.25 hours.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCPv4 Message Rate Trend</td>
<td>Every 30 minutes, starting at the 14th minute of each hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Lease History</td>
<td>39%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Threat Protection Event Count By Time (Summary)</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------</td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat Protection Event Count By Member (Summary)</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat Protection Top Rules Logged (Summary)</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat Protection Top Rules Logged by IP (Summary)</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Top Tunneling Activity (Summary)</td>
<td>Every 30 minutes, starting at every 11th and 41st minute of each hour.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS Tunneling Traffic by Category (Summary)</td>
<td>Every 30 minutes, starting at every 11th and 41st minute of each hour.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Malware and DNS Tunneling Events by Client (Summary)</td>
<td>Every 30 minutes, starting at every 11th and 41st minute of each hour.</td>
<td></td>
</tr>
<tr>
<td>Cloud</td>
<td>VM Address History (Detailed)</td>
<td>N/A</td>
<td>0%</td>
</tr>
<tr>
<td>Audit Log</td>
<td>Audit Log Events (Detailed)</td>
<td>N/A</td>
<td>0%</td>
</tr>
<tr>
<td>Ecosystem</td>
<td>Ecosystem Subscription Ecosystem Publication</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>License</td>
<td>License Pool Utilization</td>
<td>N/A</td>
<td>1%</td>
</tr>
<tr>
<td>System Utilization</td>
<td>Memory Utilization Trend (Summary)</td>
<td>Every 30 minutes, starting at the 26th minute of each half hour. Data covers the first 30 minutes of the previous 60 minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory Utilization Trend (Detailed)</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Traffic Rate (Detailed)</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Traffic Rate by Member (Summary)</td>
<td>Every 30 minutes, starting at the 28th minute of each half hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CPU Utilization Trend (Summary)</td>
<td>Every 30 minutes, starting at the top of each half hour. Data covers the first 30 minutes of the previous 60 minutes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flex Grid Licensing Features Enabled</td>
<td>Every 24 hours for all IB-FLEX members in the Grid.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** When you filter a dashboard by a time frame that is larger than the maximum retention period, the reporting server returns data within the maximum retention period. For example, when you try to view data of the CPU Utilization Trend report for the past six months, the server only returns data up to the last two months.

### Cloning Reports

1. From the **Reporting** tab, select the **Reports** tab.
2. Select the report you want to modify, click **Edit -> Clone**.
3. Enter a new title, ID, and description.
4. Set its permissions. Select Private if you do not want to share the cloned report with other users. Select Clone if you want the cloned report to have the same permissions as the original report.
5. Click Clone Report.
6. Optionally, you can do the following:
   - You can edit permissions, as described in Editing Permissions.
   - Click View to view the cloned report.
   - Click Add to Dashboard to add the cloned report to the dashboard.

Click Open in Search to open the cloned report in the Search page.

Scheduling Reports

You can schedule a report to run on a scheduled interval and trigger an action each time it runs. When scheduling a report, you can set up an action to send an email to receive report results. In addition, you can export results in CSV (comma separated value) or XML format.

To schedule a report:

1. From the Reporting tab, select the Reports tab.
2. Select the report you want to schedule, click Edit -> Schedule.

Note: You can schedule a report when you save search results as reports. When you set the paper size to A5, the logo image and report name may overlap in the footer of the downloaded reports or reports sent through email.

3. In the Edit Schedule dialog box, select the Schedule Report check box.
4. Enter the Schedule and Timerange. For more information about how to use the Schedule and Timerange options, refer to the Splunk documentation.
5. Click Next and do the following to set an action for the scheduled reports:
   - Send Email: Select this to send an email to a set of recipients to receive report results in text format, or as CSV or PDF attachments.
     - Enter the email address in the To text box. To send the email message to multiple recipients, type a comma between email addresses.

Figure 40.12 Edit Schedule

- In the Include section, select one of the following: Inline Table, Attach CSV, Attach PDF. Selecting Attach PDF or Attach CSV attaches the results of the report in the form of a CSV file or a PDF. Make sure that you specify this information.

Note: Infoblox recommends not to select Link to Report, Link to Results, Search String in the Include section. These links might not work in
Configuring Logo Image in PDF Reports

All reports display the Infoblox logo by default. You can customize reports by removing the Infoblox logo, or by replacing it with your own company logo. The reporting server uses the latest image file that you have uploaded. Make sure that you upload a logo file that is in PNG format and has a file size that is smaller than 500 KB. Note that the image file name must be pdf_logo_image.png. Do not change the logo image file name. You can configure your PDF reports and schedule to send them through emails. For information about scheduling the delivery of reports, see Scheduling Reports.

Note: In the footer of the report, you can view the logo image (if uploaded), panel name, and the timestamp when the report was downloaded. When there is no data in a single panel report, the downloaded PDF displays "No Results Found" along with "Last Updated" information. However, a report with multiple panels displays only the panel name for the panel that does not have any data.

To upload logo image:

1. From the Administration tab, select the Reporting tab -> expand the Toolbar and click Grid Reporting Properties.
   
   or
   
   From the Grid tab, select the Grid Manager tab and click the Services tab. In the Services tab, select the Reporting tab and click Edit -> Grid Reporting Properties from the Toolbar.
2. In the Grid Reporting Properties editor, select the PDF tab and complete the following:
   
   - **Logo Image**: Click Upload to open the Upload dialog box. Click Select to navigate to where the image file is located and click Open. Click Upload to upload the file. The appliance displays a preview of how it will appear on reports after you successfully upload the logo file. You can click Clear to remove the logo and upload a new one. Make sure that the file format and size meet the requirements; otherwise, the appliance displays an error message. You can click Clear to remove the uploaded image file.
3. Click Save & Close.

About Dashboards

Dashboards provide summary views for most of the data and trends in your Grid. Infoblox recommends not to modify default dashboards. To modify settings of a default dashboard, you can either clone a default dashboard, or create a new dashboard from scratch and then add panels and reports. For example, you can create a new dashboard called "DNS and DHCP Activities," and then add DNS report, add DHCP related reports, such as DHCP Top Lease Clients and DHCP Lease History, to the new dashboard. When you save the "DNS and DHCP Activities" dashboard, the reporting server saves all the reports added to the dashboard and displays dashboard with updated data. By doing this, user-defined dashboards can provide single point of access to review multiple reports that are relevant to the activities you want to monitor. If you modify a default dashboard, you can reset it to its default settings. Each dashboard comes with a set of filters to further refine report data, as described in About Dashboard Filters.

When you upgrade to 7.3.0 or later, all your system reports are migrated to Reporting tab > Dashboards.

**WARNING:** Infoblox recommends that you do not modify the predefined dashboards even if you have appropriate permissions. Editing the default dashboards changes the default settings and your changes become permanent. In addition, you might not be able to see the latest changes made by Infoblox. You can select a default dashboard and clone it to modify any of the settings, such as permissions, panels, and so on. For information, see Cloning Dashboards.

In the Dashboard panel, you can do the following using the Edit drop-down list:

- Edit panels as described in Editing Dashboards.
- Edit source, title, and description.
- Edit permissions as described in Editing Permissions.
- Clone a dashboard as described in Cloning Dashboards.
- Reset dashboards, as described in Resetting Dashboards.

Creating New Dashboards

When you add a new dashboard, Grid Manager displays it in the Reporting -> Dashboards tab. You can add multiple panels and reports to the new dashboard. For information, see Editing Dashboards.

To create a new dashboard:

1. From the Reporting tab -> select the Dashboards tab.
2. Click Create New Dashboard.
3. Complete the following:
   
   - **Title**: Enter the dashboard title.
   - **Description**: Dashboard description.
* Permissions: Click Shared in App to share a dashboard to other users. Depending on their permissions, other users can edit the dashboard. When Private is selected, the dashboard is available only to the user who creates it. You can change permissions later while editing a dashboard.

4. Click Create Dashboard.

Cloning Dashboards

It is not recommended to modify default dashboards. You can select a default dashboard and clone it to modify any of the settings, such as permissions, panels, and so on.

Note: You do not need any permission to create, modify, and delete your own personal dashboard. However, limited-access users need Read and Write permissions to modify cloned dashboards. For information about administrative permissions, see Administrative Permissions.

When you clone a dashboard, you can do the following:

- View and set permissions, as described in Editing Permissions.
- Schedule PDF delivery, as described in Scheduling PDF Delivery for Dashboards.
- Edit panels, as described in Editing Dashboards.

To create a personal dashboard:

1. From the Reporting tab, select the Dashboards tab.
2. Select the dashboard you want to modify, click Edit -> Clone.
3. Enter a new title, ID, and description.
4. Set its permissions. Select Private if you do not want to share the cloned dashboard with other users. Select Clone if you want the cloned dashboard to have the same permissions as the original dashboard.
5. Click Clone Dashboard.
6. Optionally, you can edit permissions, as described in Editing Permissions or click View to view the cloned dashboard.

Resetting Dashboards

Infoblox recommends not to modify default dashboards. However, when you make changes to the default dashboards, you can reset to its default settings.

To reset a dashboard:

1. From the Reporting tab -> select the Administration tab.
2. Click Reset Dashboards.
3. Select the check box of the dashboard or Select all to select all the dashboards.
4. Click Reset selected dashboards.

The dashboard you have modified will reset to its default settings.

Editing Dashboards

To edit the panels and filters of a dashboard, it is recommended to clone the default dashboard, and then add panels, filters and reports to the cloned dashboard. When you add a report to the panel, Grid Manager generates the corresponding dashboard in the panel. When you save the dashboard, Grid Manager updates reports in each panel. Alternatively, you can edit the XML source code to add filters and panels to a cloned dashboard, as described in Editing the XML Source Code of a Dashboard.

To add panels and filters to a dashboard:

1. From the Reporting tab -> select the Dashboards tab -> select a dashboard.
2. From the Edit drop-down list, select Edit Panels.
3. In the Edit: <Dashboard> pane, you can click Add Panel or Add Input or Edit Source.

Note: You cannot modify or delete the default values set for the dashboard filters. For example, you cannot delete or modify the filter All set for Members. When you add a new input using the editor, make sure that you edit the source and refer to the token for the input in the search string. By doing so, the search is updated when you change the input value. For information editing source, refer to Splunk documentation.

4. Optionally, you can click to delete a filter. When you delete a filter, make sure that you delete the filter information from the XML source code as well. For information, see Editing the XML Source Code of a Dashboard.

5. Expand the panel categories and select the panel you want to add. For detailed information about how to add panel categories, refer to the Splunk documentation.

6. Click Add to Dashboard.
Editing the XML Source Code of a Dashboard

**Note:** Before editing dashboards, forms, and panel files in simple XML source code, you should be familiar with the basic layout of dashboards and the XML elements that define them. Infoblox recommends that you save a copy of the source code of the dashboard before making any modifications.

To edit the XML source code for a dashboard:

1. From the **Reporting** tab, select the **Dashboards** tab.
2. Select a dashboard you want to edit the XML source code, click **Edit -> Edit Source**.

You can add filters, such as check box, drop-down list, radio button, and text box. For information about how to edit the XML source code, refer to the Splunk documentation.

Example - Adding an extensible attribute filter

If your reporting data contains the "location" extensible attributes associated to members, adding the following sample XML code to the XML source code will create an extensible attribute filter, **Member Location**:

```xml
<input type="dropdown" token="ea_location">
  <label>Member Location</label>
  <choice value="All">All</choice>
  <default>All</default>
  <search>
    <query> | inputlookup __grouping_by_ea_tag_lookup 
      | spath input=EA path=Location output=EA_Location 
      | stats count by EA_Location </query>
    <earliest>$time.earliest$</earliest>
    <latest>$time.latest$</latest>
  </search>
  <fieldForLabel>EA_Location</fieldForLabel>
  <fieldForValue>EA_Location</fieldForValue>
  <change>
    <condition value="All">
      <set token="ea_location_str"> | noop </set>
    </condition>
    <condition value="*">
      <set token="ea_location_str"> | spath input=EA path=Location output=EA_Location 
        | where EA_Location="$value$" </set>
    </condition>
  </change>
</input>

<search id="base_search">
  <query>index=ib_system_summary report=si_cpu_usage
    $members$
    $ea_site_str$
</query>
</search>
```
The generated PDF appears in a browser window. You can view, download, or print the PDF from the browser window. A single dashboard PDF includes up to 1,000 rows of table data.

Do the following to print a dashboard:

1. From the Reporting tab, select the Dashboards tab -> select a dashboard.
2. Click Print. The default print driver for your browser opens with print settings.

### Scheduling PDF Delivery for Dashboards

To schedule PDF delivery for dashboards, you must first create a new dashboard. Ensure that email notification settings are configured prior to scheduling PDF delivery. For information, see Configuring Email Notification Settings. To schedule PDF delivery, you can use the dashboard Edit drop-down list. You can access the Edit drop-down list directly from a dashboard or from the Dashboards page.

**Note:** Scheduled PDF delivery is not available for dashboards that include forms.

Do the following if the Schedule PDF Delivery option is disabled:

1. Open the dashboard for which you want to schedule PDF delivery.
2. Click Open in Search icon available at the bottom of the dashboard panel.
3. From the Save As menu, click Dashboard Panel.

To set up PDF delivery for the dashboard with a single panel:

1. From the Reporting tab, select the Dashboards tab.
2. Do one of the following:
   - Select the dashboard you want to schedule, click Edit -> Schedule PDF Delivery. If the Schedule PDF Delivery option is disabled, follow the steps as described above.
   - Open the dashboard in the Dashboards page and click Schedule PDF Delivery from the Edit drop-down list.
3. In the Edit PDF Schedule dialog box, do the following:
   - Select the Schedule PDF Delivery check box to enable PDF delivery.
   - Select a schedule. For more information, refer to the Splunk documentation.
   - In the Email To text box, specify email address.
   - Select paper size and paper layout. You can change the paper size and paper layout, if data is not displayed properly in the PDF delivery.
   - To receive dashboard PDFs immediately, click Send Test Email.
4. Click Save.

**Note:** To set up PDF delivery for the dashboard with multiple panels, repeat the above steps from step 1 to step 4 and add other panels to the dashboard created for the first panel.

*Figure 40.13 Edit PDF Schedule dialog box*
About Dashboard Filters

You can apply different filters to control the data displayed in the dashboards. The data on the dashboard is displayed based on the various filter criteria you select.

To apply a filter:

1. From the Reporting tab, select the Dashboards tab -> select a dashboard.
2. Apply filter criteria appropriately and click Submit.
   The dashboards display results based on the filters that you apply.

The most common filters are as follows:

- **Time**
- **Top N**: Top most filter options. The default is 10. You can select from a set of fixed values for the TopN filter setting: 5, 10, 20, 50, 100, 200, 250, or 500.
- **Members**: Grid members configured on the appliance.
- **Network**
- **Member Site**, as described in Applying Extensible Attribute Filters.

Applying Time Filters
You can generate a dashboard for a specific time interval by applying time filters. You can filter results by preset time ranges, create custom time ranges, specify time ranges based on dates or date and time, or work with advanced features in the time range picker. For information about Time range picker, refer to the Splunk documentation.
The date and time displayed in the Time filters are based on the time zone set in your user profile by default. For more information about how to configure a time zone, see Setting the Browser Time Zone. However, the timestamp displayed in the results for a dashboard is based on the time zone configured on the reporting server.

**Note:** The NIOS reporting data is updated at a certain time interval, rather than updating continuously. Therefore, the Real-time option in the Time filter might not work for most of the dashboards. For information about update time intervals, see Reporting Indexes and Update TimeIntervals.

### Applying Extensible Attribute Filters

You can use extensible attribute filters to narrow down the search by including only members that contain certain extensible attribute values. An extensible attribute added to a member is displayed in the Extensible Attribute filter. For information about managing extensible attributes, see About Extensible Attributes. When you configure group-by-extensible-attribute search and apply the Extensible Attribute filter, the dashboard displays results for grouped members that have the same extensible attribute value for the Site extensible attribute. If you have configured multiple attribute values for a member, then applying the Extensible Attribute filter displays all the attribute values associated with that member. For example, if member 1 has predefined attribute Site with attribute values member a and member b and member 2 has predefined attribute Site with attributes values member c and member d, then the dashboard displays member a and member b when you apply the Member Site < member 1 > filter.

In addition, you can apply Group By EA Tag filter and group members with the same extensible attribute value so that instead of displaying data per member, the reports display data per group of members with the same value for the Site extensible attribute. When you apply Group By EA Tag filter, you can set the data calculation method to decide which statistic value [Aggregate, Average, or Maximum] you want to be displayed for grouped members. You can group by Active Directory Sites for the IPAMv4 Network Usage Statistics report, IPAMv4 Top Utilized Networks report, and DHCPv4 Network Usage Statistics report.

To apply an extensible attribute and group by EA tag/field filters:

1. From the Reporting tab, select the Dashboards tab -> select a dashboard.
2. In the filter section, complete the following:
   - **Member <Extensible Attribute>:** Select an extensible attribute configured for a member. If you need an additional extensible attribute filter, you must first clone the default dashboard, and then add an extensible attribute filter by editing the XML source code. For information, see Editing the XML Source Code of a Dashboard.
   - **Group By EA Tag/Field:** Select an extensible attribute to enable the reporting server to group networks by members that have certain extensible attribute tags or fields. Note that this option is available for specific dashboards only.

**Note:** If you use special characters in the extensible attribute name, the appliance replaces these special characters with equivalent values. For example, if you add the extensible attribute Site In London, it is displayed as Site20In20London in the Group By EA Tag/Field drop-down list. In this example, space is replaced with 20. If you add the extensible attribute London@, it is displayed as London40 in the Group By EA Tag/Field drop-down list.

- **Calculation Methods:** This field is enabled only when you select the Group by EA Tag/Field check box. The displayed result varies based on your search definitions. The result values can contain information such as event counts, DNS queries, traffic rate, and usage trends. For example, when you select Maximum, the DNS Query Rate by Member dashboard shows all the members that have the same extensible attributes and members with the maximum DNS queries, and the Threat Protection Event Count By Member dashboard shows the members that have the same extensible attributes and maximum event counts. Select one of the following methods:
  - **Aggregate:** Displays the sum of values for individual members in a group.
  - **Average:** Displays the mathematical average of a group. This value is obtained by adding values for all members in a group and then dividing the total by the number of members.
  - **Maximum:** Displays the maximum value among the members in a group.

**Note:** When you apply Group By EA Tag/Field in Active Directory Sites supported reports, the values displayed in these reports are aggregated sum of absolute values (sum of values of individual networks in a group) and utilization% is the mathematical average of the group.

You can configure the group-by-extensible-attribute filter and data calculation methods for the following dashboards only:

- CPU Utilization Trend (Detailed)
- IPAMv4 Network Usage Statistics
- IPAMv4 Top Utilized Networks
- IPAMv4 Network Usage Trend
- DDNS Update Rate Trend
- DHCPv4 Usage Statistics
- DNS Daily Query Rate by Member
- DNS Query Rate by Member
- DNS Daily Peak Hour Query Rate by Member
- DNS Response Latency Trend
- DNS Cache Hit Rate Trend
- DNS Traffic Control Resource Availability Trend

Copyright ©2019, Infoblox, Inc. All right reserved.
Predefined Dashboards

Table 40.9 lists the dashboard categories and their corresponding dashboard. You can apply filters and view the dashboards in table, stacked area, or in both the view.

**Table 40.9 Dashboard Categories**

<table>
<thead>
<tr>
<th>Dashboard Category</th>
<th>Corresponding Dashboard</th>
<th>Displays IDNs in Punycode (Yes/No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Log Events</td>
<td>Audit Log Events</td>
<td>Yes</td>
</tr>
<tr>
<td>IPAMv4 Utilization</td>
<td>DHCPv4 Top Utilized Networks</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>DNS Statistics per DNS View</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>DNS Statistics per Zone</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>IPAMv4 Network Usage Statistics</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>IPAMv4 Network Usage Trend</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>IPAMv4 Top Utilized Networks</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>DNS Object Count Trend for Flex Grid License</td>
<td>NA</td>
</tr>
<tr>
<td>Devices (Discovery)</td>
<td>Inactive IP Addresses</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Port Capacity Delta by Device</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Port Capacity Trend</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Port Capacity Utilization by Device</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>IP Address Inventory</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Network Inventory</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>End Host History</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Device Interface Inventory</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Device Inventory</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Device Components</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>IPAMv4 Device Networks</td>
<td>Yes</td>
</tr>
<tr>
<td>DHCP Dashboards</td>
<td>DHCP Dashboards</td>
<td>Yes</td>
</tr>
<tr>
<td>DHCP Fingerprints</td>
<td>Device Trend</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Device Class Trend</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Top Devices Identified</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Top Devices Denied an IP Address</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Top Device Classes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Device Fingerprint Change Detected</td>
<td>Yes</td>
</tr>
<tr>
<td>DHCP Lease</td>
<td>DHCP Lease History</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>DHCP Top Lease Clients</td>
<td>IDN is not supported</td>
</tr>
<tr>
<td>Category</td>
<td>Dashboard</td>
<td>Available</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td><strong>DHCP Performance</strong></td>
<td><strong>DHCPv4 Range Utilization Trend</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DHCPv4 Range Utilization Trend</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DHCPv4 Usage Trend</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DHCP Message Rate Trend</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>DNS Dashboards</strong></td>
<td><strong>DDNS Query</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>DDNS Update Rate Trend</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Performance</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>DNS Response Latency Trend</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Effective Peak Usage Trend for Flex Grid License</strong></td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Query</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>DNS Top Requested Domain Names</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Top Clients</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Top Clients Per Domain</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Query Rate by Query Type</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Query Rate by Member</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Replies Trend</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Response Latency Trend</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Top Clients Per Domain</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Top NXDOMAIN / NOERROR (no data)</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Top SERVFAIL Errors Sent</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Top SERVFAIL Errors Received</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Top Timed-out Recursive Queries</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Query Trend per IP Block Group</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Security Dashboards</strong></td>
<td><strong>FireEye Alerts</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Top RPZ Hits</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Top RPZ Hits by Clients</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Threat Protection Event Count By Severity Trend</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Threat Protection Event Count By Member Trend</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Threat Protection Event Count By Rule</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Threat Protection Event Count By Time</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Threat Protection Event Count By Category</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Threat Protection Event Count By Member</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Threat Protection Top Rules Logged</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Threat Protection Top Rules Logged by Source</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Top Tunneling Activity</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Tunneling Traffic by Category</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Top Malware and DNS Tunneling Events by Client</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Ecosystem Dashboards</strong></td>
<td><strong>User Login History Report</strong></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Subscription Data</strong></td>
<td>Yes</td>
</tr>
</tbody>
</table>
Audit Log Events
The Audit Log Events dashboard provides information about the administrator-initiated events such as login events, logout events, service restarts, appliance reboots, write operations such as the addition, modification, and deletion of objects, etc. The default dashboard displays the audit log events for all admin users and for all Grid members in table format. You can use the displayed fields as filters to get specific information you want displayed in the dashboard. Only superusers can view and modify this dashboard.
This dashboard displays the following information about each audit log event in table format:

- **Timestamp**: The date, time, and time zone the task was performed. The time zone is the time zone configured on the member.
- **Admin**: The admin user who performed the task.
- **Action**: The action performed. This can be one of the following: Called, Created, Deleted, Login_Allowed, Login_Denied, Message, Modified, and Logout.
- **Object Type**: The object type of the object involved in this task.
- **Object Name**: The name of the object involved in this task.
- **Execution Status**: The execution status of the task. Possible values are Executed, Normal, Pending Approval, and Scheduled.
- **Message**: Detailed information about the performed task.
- **Members**: The Grid member on which the task was performed.

IPAMv4 Utilization Reports

DHCPv4 Top Utilized Networks
The DHCPv4 Top Utilized Ranges dashboard provides statistics about the top most utilized DHCPv4 networks. The default dashboard includes the top 10 most utilized DHCPv4 networks within the last 24 hours.
This dashboard displays the following information in table format:

- **Timestamp**: The date and time of the recorded utilization.
- **Network View**: The network view.
- **Network**: The network address.
- **CIDR**: The subnet mask in CIDR format.
- **DHCPv4 Utilization%**: The percentage of DHCP addresses in use over the total number of DHCP addresses provisioned.
- **Ranges**: The number of DHCP address ranges in the network.
- **Provisioned**: The total number of IP addresses in the range.
- **Dynamic**: The number of dynamic IP addresses in the range.
- **Static**: The number of static IP addresses in the range.
- **Free**: The number of free DHCP addresses.
- **Used**: The total number of IP addresses in use.

DNS Statistics per DNS View
The DNS Statistics per DNS View dashboard provides DNS zone statistics for each DNS view in a given time frame. The default dashboard includes information for all network views, all members, all IPv4 and IPv6 reverse-mapping zones, all forward-mapping zones, and all DNS records by record type.
This dashboard displays the following information in table format:

- **Timestamp**: The date and time of the event.
- **View**: The DNS view.
- **Members**: The FQDN of the member that is associated with the DNS view.
- **Forward-Mapping Zone**: The number of forward-mapping zones.
IPv4 Reverse-Mapping Zone: The number of IPv4 reverse-mapping zones.
Signed Zone: The number of signed zones.
Host: The number of host records.
LBDN: Number of LBDNs assigned to the zone. Note that if an LBDN is assigned to multiple zones or views, the appliance displays it separately for each zone or view.
Total Records: The total number of DNS resource records.

Grid Manager also displays the number of each relevant DNS resource records.

DNS Statistics per Zone

Since every DNS view can have multiple zones and each zone can have multiple records, this dashboard highlights the list of all zones and provides statistics based on every DNS Zone. This dashboard allows you to identify how many and what type of DNS records each zone is serving and use these statistics for more effective planning. The DNS Statistics per Zone displays the following information:

- Timestamp: Timestamp of events.
- Zone: FQDN of zone.
- Signed: Boolean to indicate if the zone is signed.
- Hosts: Number of hosts.
- LBDN: Number of LBDNs assigned to the zone. Note that if an LBDN is assigned to multiple zones or views, the appliance displays it separately for each zone or view.
- Total Records: Number of total resource records, Host are not counted.
  - A Records: number of A records.
  - AAAA Records: number of AAAA records.
  - CNAME Records: number of CNAME records.
  - DNAME Records: number of DNAME records.
  - DNSKEY Records: number of DNSKEY records.
  - DS Records: number of DS records.
  - MX Records: number of MX records.
  - NAPTR Records: number of NAPTR records.
  - NSEC Records: number of NSEC records.
  - NSEC3PARAM Records: number of NSEC3PARAM records.
  - NSEC3 Records: number of NSEC3records.
  - NS Records: number of NS records.
  - PTR Records: number of PTR records.
  - RRSIG Records: number of RRSIG records.
  - SOA Records: number of SOA records.
  - SRV Records: number of SRV records.
  - TXT Records: number of TXT records.
  - Other Records: number of other records.

IPAMv4 Network Usage Statistics

The IPAMv4 Network Usage Statistics dashboard provides usage statistics for each network in a given time frame. This dashboard displays the following information in table format:

- Timestamp: The timestamp when the network container was created.
- Network: The network address.
- Network View: The network view.
- CIDR: The subnet mask in CIDR format.
- AD Site: The Active Directory Site associated with the network. For networks that are not associated with Active Directory Domains and Sites, or when you delete an Active Directory server, the appliance displays no_value in this column.
- DHCPv4 Utilization%: The percentage of DHCP addresses in use over the total number of DHCP addresses provisioned.
- Total: The total number of IPAM addresses in the network.
- Allocated: The number of allocated IP addresses in the network.
- Reserved: The number of reserved IP addresses in the network.
- Assigned: The number of assigned IP addresses in the network.
- Utilization%: The percentage of IP address in use over the total number of IP addresses in the network.
- Unmanaged: The number of discovered IP addresses that do not have corresponding records on the appliance, such as A records, PTR records, fixed address records, host records, or leases.

IPAMv4 Network Usage Trend
The **IPAMv4 Network Usage Trend** dashboard provides IPAM usage trends for the network utilization in specific Active Directory Sites over time. Each of the line graphs is represented with a different color. This is a detailed report only. You can aggregate the report based on the networks or Active Directory Sites. This dashboard displays the following information:

- **Time**: The timestamp of the event.
- **Usage%**: The percentage of IPAM address network usage.

**IPAMv4 Top Utilized Networks**

The **IPAMv4 Top Utilized Networks** dashboard provides statistics about the top most utilized IPv4 networks. The default dashboard includes the top 10 most utilized networks within the last hour. This dashboard displays the following information in table format:

- **Timestamp**: The date and time of the recorded utilization.
- **Network View**: The network view.
- **Network**: The network address.
- **CIDR**: The subnet mask in CIDR format.
- **ADSite**: The Active Directory Site associated with the network. For networks that are not associated with Active Directory Domains and Sites, or when you delete an Active Directory server, the appliance displays **no_value** in this column.
- **DHCPv4 Utilization%**: The percentage of IP address in use over the total number of IP addresses in the network.
- **Total**: The total number of IP addresses in the network.
- **Assigned**: The total number of IP addresses assigned in the network.
- **Reserved**: The total number of reserved IP addresses in the network.
- **Unmanaged**: The number of discovered IP addresses that do not have corresponding records on the appliance, such as A records, PTR records, fixed address records, host records, or leases.

**DNS Object Count Trend for Flex Grid License**

The **DNS Object Count Trend for Flex Grid License** dashboard lists the average DNS object count across all IB-FLEX members in the Grid during the past five days. The DNS object count is calculated as the total DNS resource record count for all DNS zones with IB-FLEX member as the Grid primary. The data is generated once every 24 hours and the average is calculated over 5 days. This dashboard displays the following information in either line chart or table format:

- **Show Filters**: Click **Show Filters** to enable the filters.
- **Time**: Select a value from the drop-down list. The default value is **Last 6 days**.
- **Line Chart**: Click **Line Chart** to view the data in line chart format.
- **Table**: Click **Table** to view the data in table format.
- **Both**: Click **Both** to view the data in both line chart and table format.

**Device (Discovery) Dashboards**

**Inactive IP Addresses**

The **Inactive IP Addresses** dashboard lists inactive IP addresses that are not in use since the initial specified time, and remain so through the last discovery cycle. For example, you can use this dashboard to compare the state of all ports on devices for one month's operation versus 1 week's operation. The dashboard lists inactive IP addresses associated with Hosts, IPv4 and IPv6 Fixed Address objects, and IPv4 Reservation objects. Each unique IP address within each network view appears exactly once in the dashboard. You can go to the **Data Management → IPAM** page to delete listed inactive IP addresses.

By default, this dashboard operates for all devices across all network views. This dashboard supports use of a single time filter. You can filter by device name or network view.

This dashboard displays the following IP address and device information in table format:

- **IP**: The IP address.
- **Last MAC/DUID**: The discovered MAC or DUID.
- **Type**: Inactive IP address object type: Fixed Address, IPv4 Reservation or Host.
- **Device Type**: The type of device connected to the inactive IP address. Types include **Router**, **Firewall**, **Switch-Router**, and **Switch**.
- **Device Name**: The name of the device connected to the inactive IP address.
- **Port/Interface**: The device interface bound to the IP address.
- **Network View**: The network view containing the inactive IP address.

**Port Capacity Delta by Device**

The **Port Capacity Delta by Device** dashboard provides three Start/End time ranges by which each measured device illustrates how many interfaces move into and out of the three key functional states for each port: Administratively Up/Operationally Up, Administratively Up/Operationally Down and Administratively Down/Operationally Down.
For example, consider a port that is in the Administratively Up/Operationally Up status on a given device at the beginning of a one-week measurement (Start), and that it is the only port that changes state for that device in the measurement period. At the end of the measurement period (End) it goes into an Administratively Up/Operationally Down state. At first, the Administratively Up/Operationally Up Start counter reflects the discovered state at the beginning of the measurement period. When the port changes state, and its change is discovered, the Administratively Up/Operationally Up End counter decrements by 1; the Administratively Up/Operationally Down Start counter increases by 1. The data format is similar to the Port Capacity Utilization by Device report except that each data point divides into two values (Start and End), reflecting the delta.

You can filter by device name or network view, or both. This dashboard displays the following categories of information in table format:

- **Device Name**: Name of the listed device.
- **Admin Up, Operation Up Start**: count at the starting time of measurement of device interfaces in Admin Up/Operational Up status.
- **Admin Up, Operation Up End**: count at the ending time of measurement device interfaces in Admin Up/Operational Up status.
- **Admin Down, Operation Down Start**: count at the starting time of measurement of device interfaces in Admin Down/Operational Down status.
- **Admin Down, Operation Down End**: count at the ending time of device interfaces in Admin Down/Operational Down status.
- **Admin Up, Operation Down Start**: count at the starting time of measurement of device interfaces in Admin Up and Operational Down status.
- **Admin Up, Operation Down End**: count at the ending time of device interfaces in Admin Up and Operational Down status.
- **Total Available**: The total number of available ports for the listed device.
- **Network View**: The grid Manager Network View to which the device is associated.

**Port Capacity Trend**

The Port Capacity Trend report is a line graph of device port utilization over time. It uses the Administratively Up/Operationally Up, Administratively Up/Operationally Down, and Administratively Down/Operationally Down counters; by default, for all interfaces across all devices, across all network views, to produce a line chart illustrating four broad data categories:

- **Admin Up, Operation Up**: cumulative count over time of device interfaces in Admin Up/Operational Up status.
- **Admin Down, Operation Down**: cumulative count over time of device interfaces in Admin Down/Operational Down status.
- **Admin Up, Operation Down**: cumulative count over time of device interfaces in Admin Up and Operational Down status.
- **Total Available**: Total number of ports on all devices across all network views, whether provisioned or not.

The default time span for this trend chart is one week of measurement. You can filter by device name or network view, or both. You will need to know the device name or network view name for filter entry.

Should you turn off filtering, the dashboard shows the collected data "for all time;" for the entire period since monitoring began.

**Port Capacity Utilization by Device**

The Port Capacity Utilization by Device provides the devices' overall port status for the specified time, without stating devices' or individual ports' operating state. Each device's count of unused interfaces, within each network view, appears exactly once in the dashboard. By default, the table sorts by ascending Device Name. By default, this dashboard lists all devices, across all network views. You can filter by device name or network view, or both. Grid Manager takes snapshots of data for Port Capacity reports every six hours.

You will see three distinct port configuration combination counts per device:

- Administratively Up, Operationally Up
- Administratively Up, Operationally Down
- Administratively Down, Operationally Down

This dashboard displays the following information in table format:

- **Device Name**: The name of the device associated with the port status counts.
- **Admin Up, Operation Up**: The count of device interfaces in Admin Up/Operational Up status.
- **Admin Down, Operation Down**: The count of device interfaces in Admin Down/Operational Down status.
- **Admin Up, Operation Down**: The count of device interfaces in Admin Up and Operational Down status.
- **Total Available**: Total number of interfaces available for the device, whether provisioned or not.
- **Network View**: The network view containing the listed device.

**IP Address Inventory**

The IP Address Inventory dashboard provides information about all IP addresses that can be discovered by NetMRI (IPAM sync), vDiscovery, and Network Insight solutions. This dashboard displays the list of IP addresses, management platform, discovered name, and the details of the network devices that have been discovered.

The dashboard data can be filtered by Time, Network View, IP Address, Management Platform, First Seen and Last Seen timestamps. For instance, you can filter by Management Platform and see which platform the device possesses during the given time frame.

- **IP address**: The discovered IPv4 or IPv6 address.
- **Discovered Name**: The discovered name of the device.
- **First Seen**: The timestamp when the IP address was first seen in the network.
- **Last Seen**: The timestamp when the IP address was last seen in the network.
- **Network View**: The network view with which the IP address is associated.
- **Managed**: Indicates if the discovered device is managed by NIOS. For NIOS managed device, you can define basic characteristics and manage those devices on NIOS.
- **Management Platform**: The platform information from where IP address is discovered. This can be Network Insight, Amazon, OpenStack, or VMware.
- **VLAN Name**: The VLAN name on the switch port.
- **VLAN ID**: The VLAN ID on the switch port.

### Network Inventory

The **Network Inventory** dashboard provides information about all known networks. The dashboard displays the list of device IP addresses, IP address utilization%, management platform, and the netmask details of the devices that have been discovered. This dashboard displays a table that contains the following information:

- **Device IP Address**: The IP address of the device.
- **Netmask**: The netmask of the network.
- **First Seen**: The timestamp when the IP address was first seen in the network.
- **Last Seen**: The timestamp when the IP address was last seen in the network.
- **Network View**: The network view with which the device is associated.
- **Utilization%**: Displays the percentage based on the IP addresses that are currently in use on the network. For example, a /30 subnet mask can have two IP addresses that are in use. If both IP addresses are detected then the Utilization% is 100%.
- **Managed**: Indicates whether this network is a managed or unmanaged object in NIOS. Managed objects are configured for DNS or DHCP and have corresponding NIOS objects such as fixed addresses, DNS records, or host records, which you can manage directly in NIOS.
- **Management Platform**: The platform information from where IP address is discovered. This can be Network Insight, Amazon, OpenStack, or VMware.
- **VLAN ID**: The VLAN ID on the switch port.
- **VLAN Name**: The VLAN name on the switch port.

### Network Insight Dashboards

The Network Insight dashboards are available only when you have configured the Network Insight appliance as a Grid member with a valid Network Insight license installed. For information about Network Insight, see [Infoblox Network Insight](https://www.infoblox.com/products/network-insight).

### End Host History

The **End Host History** dashboard provides the history of the end hosts discovered by Network Insight in a given time frame across all network views. This dashboard is applicable only for the Network Insight solution. The dashboard displays the list of MAC addresses for end hosts, their IP addresses and the details of the network devices from which the end hosts have been discovered. The dashboard data can be filtered by Network View, MAC Address, IP Address, First Seen and Last Seen timestamps. For instance, you can filter by MAC address and see which IP address the end host possesses during the given time frame. You can also filter by the First Seen and/or Last Seen timestamp and find the MAC addresses of the end hosts becoming active and/or going offline. This dashboard displays the following information in table format:

- **MAC Address**: The MAC address of the end host.
- **IP address**: The IP address of the end host.
- **First Seen**: The timestamp when the MAC address was first seen in the network.
- **Last Seen**: The timestamp when the MAC address was last seen in the network.
- **Network View**: The network view with which the end host is associated.
- **Device Name**: The name of the network device that has the ARP (Address Resolution Protocol) of the end host.
- **Device Vendor**: The vendor of the network device that has the ARP of the end host.
- **Device Model**: The model of the network device that has the ARP of the end host.
- **Device OS Version**: The OS version of the network device that has the ARP of the end host.
- **Device Interface**: The interface name of the network device that has the ARP of the end host.
- **Device VLAN**: The VLAN ID of the interface that has the ARM (Asynchronous Response Mode) of the end host.
- **AP Name**: The name of the access point of the device. This column is displayed only for wireless devices.
- **AP IP Address**: The IP address of the access point of the device. This column is displayed only for wireless devices.
- **SSID**: The unique name of the WLAN (Wireless Local Area Network).
- **User Name**: The name of the user. This column is displayed only when the Identity Mapping feature on the appliance is enabled. For information about how to enable the Identity Mapping feature, see [Enabling Identity Mapping](https://www.infoblox.com/products/network-insight).

### Device Interface Inventory

The **Device Interface Inventory** dashboard provides interface statistics of devices discovered by Network Insight in a given time frame. This dashboard is applicable only for the Network Insight solution. The dashboard displays the list of interface IP addresses, device operating system, device model, discovered name, and the details of the network devices that have been discovered. This dashboard displays a table that contains the following information:
• **Network View**: The network view to which the device is associated.
• **Device IP Address**: The IP address of the network device.
• **Device Name**: The name of the network device.
• **Device Type**: The device type as discovered. This can be **Switch**, **Router**, or **Switch-Router**.
• **Device Vendor**: The vendor of the network device.
• **Device Model**: The model of the network device.
• **Device OS Version**: The OS version of the network device.
• **Interface Name**: The interface name of the network device.
• **Interface IP**: The IP address of the device interface.
• **Interface Description**: Additional information about the device interface.
• **Admin Status**: The switched interface's Admin status (whether the port is administratively enabled by the operator).
• **Operation Status**: The switched interface's operating status.
• **Last Port Changed**: The timestamp of the last change made on the interface (change can be anything such as changing the description, changing the VLAN, or changing the interface status to up or down).
• **Trunk Port**: Indicates if the interface is enabled for trunking (allows multiple VLANs). Displays **Yes** or **No**.
• **Type**: The standard interface type supported by the port.
• **Speed**: The line speed of each listed interface.
• **VLAN ID**: The VLAN ID on the switch port.
• **VLAN Name**: The VLAN name on the switch port.
• **Network**: The network address.

**Device Inventory**

The **Device Inventory** dashboard provides statistics of device inventory data discovered by Network Insight in a given time frame. This dashboard is applicable only for the Network Insight solution. The dashboard displays the list of interface IP addresses, device operating system, device model, discovered name, and the device details that have been discovered. This dashboard displays a table that contains the following information:

• **Device Type**: The device type as discovered. This can be **Switch**, **Router**, **Firewall**, **Load Balancer**, **Switch-Router** and so on.
• **Asset Type**: Indicates that the device is a physical device, virtual device, or host.
• **Device Vendor**: The vendor of the device.
• **Device Model**: The model of the device.
• **OS Version**: The version of the operating system that is running on the device.
• **Device Name**: The name of the device.
• **Chassis S/N**: Displays the hardware serial number. This displays multiple values if there are more than one chassis or modules installed on the hardware.
• **Device IP Address**: The IP address of the network device.
• **Network View**: The network view with which the device is associated.
• **First Seen**: The timestamp when the IP address was first seen in the network.
• **Last Seen**: The timestamp when the IP address was last seen in the network.

**Device Components**

The **Device Components** dashboard provides information about device components discovered by Network Insight. This dashboard is applicable only for the Network Insight solution. The dashboard displays the list of device IP addresses, device operating system version, device model, device vendor, discovered name, and the device model that have been discovered. This dashboard displays a table that contains the following information:

• **Device IP**: The IP address of the device.
• **Network View**: The network view with which the device is associated.
• **Device Name**: The name of the device.
• **Device Model**: The model of the device.
• **Device Vendor**: The vendor of the device.
• **OS Version**: The version of the operating system that is running on the device.
• **Name**: The name of the network component.
• **Description**: Additional information about the network component.
• **Class**: The device category.
• **S/N**: Displays the hardware serial number. This displays multiple values if there are more than one chassis or modules installed on the hardware.
• **Model**: The product name or model of the network device.
• **Hardware Rev**: The hardware version number of the device.
• **Firmware Rev**: The firmware version of the device.
• **Software Rev**: The software version of the device.

**IPAMv4 Device Networks**

The **IPAMv4 Device Networks** dashboard provides IPAMv4 device usage for each network in a given time frame. This dashboard displays the following information:
- **IPAM Network**: The network address.
- **Utilization %**: The percentage of IP address in use over the total number of IP addresses in the network.
- **Network View**: The network view.
- **Device IP**: The IP address of the device.
- **Device Name**: The name of the device.
- **Interface IP**: The IP address of the device interface.
- **Device Model**: The model of the device.
- **Device Vendor**: The vendor of the device.
- **Device OS Version**: The version of the operating system that is running on the device.

### DHCP Dashboards

#### Device Class Trend

The *Device Class Trend* dashboard provides trends for the top device classes used by remote clients in a given time frame. The default dashboard displays line graphs for the top device classes used by remote clients over the last 24 hours. Each of the device class is represented with a different color line graph.

#### Device Fingerprint Change Detected

The *Device Fingerprint Change Detected* dashboard provides information about the devices whose fingerprint data gets changed in a given time frame. In other words, this dashboard includes all devices used by remote clients that were detected to have the same Mac address but different device class in a given time frame. The following example illustrates how the fingerprint data can change in a given time frame:

A client device having dual boot option may request for an IP address while switching between operating systems, resulting in a change of fingerprint data and if a client's device uses Mac Boot Camp, the mac address remains unchanged, but fingerprint data changes when it switches operating system.

*Note*: The *Device Fingerprint Change Detected* report includes all devices whose fingerprint data has been changed within the last seven days. It ignores devices whose fingerprint data has been changed for more than seven days.

This dashboard displays a table that contains the following information:

- **Time**: The time the lease was obtained.
- **Mac/DUID**: The Mac address or DUID of the client's device.
- **Current Device Type**: The current fingerprint description of the device.
- **Current Device Class**: The current fingerprint class of the device.
- **Previous Device Type**: The fingerprint description of the device before changing the fingerprint data.
- **Previous Device Class**: The fingerprint class of the device before changing the fingerprint data.
- **Action**: The current status of the lease. The lease status can be one of the following: *Issued*, *Renewed*, *Freed*, or *Abandoned*.

#### Device Trend

The *Device Trend* dashboard provides trends for the top operating systems used by remote clients in a given time frame. The default dashboard displays line graphs for the top 10 operating systems used by remote clients over the last 24 hours. Each of the operating system is represented with a different color line graph. For more information about DHCP fingerprint detection, see *About DHCP Fingerprints*.

### DHCP Lease History

The *DHCP Lease History* dashboard provides DHCP lease history in a given time frame. The search of the DHCP Lease History report is scheduled hourly by default. DHCP Lease History reports can impose heavier system loads than for other alert types in the NIOS system. Avoid defining too many personal reports or alerts of this type for Grid reporting. Other types of reports do not impose significant performance restrictions. Also see *About IP Blocks and IP Block Groups* for methods to avoid this issue. You can drill down to the IP address of the lease and view user history for the selected IP address.

*Note*: When you join a new member to the Grid and do not start reporting service on the member, lease history for this member is not captured in the *DHCP Lease History* report. You can view lease history for this member in the *Data Management* tab -> *DHCP* tab -> *Leases* tab.

The default dashboard displays the following information in table format:

- **Time**: The timestamp when the lease information was updated.
- **Members**: The DHCP member that granted the lease.
- **Member IP**: The IP address of the DHCP member that granted the lease.
• **Lease IP**: The IP address of the lease. You can click the lease IP address to view login details of the user. For information about User History for Lease IP sub-report, see User History for Lease IP. You can also view subscription data for the selected lease IP. For information, see Subscription Data.

• **Protocol**: Indicates whether the lease is for an IPv4 or IPv6 address.

• **Action**: The status of the lease. This can be one of the following: Issued, Renewed, Freed, or Abandoned.

• **Hostname**: The host name that the DHCP client sent to the appliance using DHCP option 12.

• **MAC/DUID**: For an IPv4 address, this is the MAC address of the lease. For an IPv6 address, this is the DUID (DHCP Unique Identifier) of the DHCP client that received the lease.

• **Lease Time**: The lease time of the DHCP client.

**Note**: Some of the options in the Lease Time filter might not display any data.

• **Lease Start**: The start date of the lease.

• **Lease End**: The end date of the lease.

• **Fingerprint**: The name of the DHCP fingerprint or vendor ID of the leased client that was identified through DHCP fingerprint detection. This field displays No Match for devices that do not match the filter criteria and those that do not have any DHCP fingerprint information. For information about DHCP fingerprints, see About DHCP Fingerprints.

• **Component Name**: The name of the device.

• **Component Port**: The port or interface connected to the device.

• **Device Class**: Filter by the device category to which the leased client belongs.

**DHCP Message Rate Trend**

The **DHCP Message Rate Trend** dashboard provides the overall DHCP message rate trends for DHCP message types in a given time frame. The default dashboard displays the actual, maximum, average, and minimum rate trends in the last 24 hours for the following message types: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, and DHCPACK.

This dashboard displays the following information:

• **Time**: The timestamp of the event.

• **DHCPDISCOVER**: The actual rate trend of the DHCPDISCOVER messages.

• **DHCPOFFER**: The actual rate trend of the DHCPOFFER messages.

• **DHCPREQUEST**: The actual rate trend of the DHCPREQUEST messages.

• **DHCPACK**: The actual rate trend of the DHCPACK messages. Each of the line graphs is represented with a different color.

**DHCP Top Lease Clients**

The **DHCP Top Lease Clients** dashboard provides information about the DHCP clients that have issued, renewed, and freed within a certain time frame.

This dashboard shows the following information:

• **MAC/DUID**: The MAC address or DUID of the DHCP client.

• **Issued**: The total number of DHCP lease issued.

• **Renewed**: The number of DHCP lease renewals.

• **Freed**: The number of leases that were released.

• **MAC/DUID Total**: The total number of DHCP leases that were being requested, renewed, and released.

• **Fingerprint**: The name of the DHCP fingerprint or vendor ID of the leased client that was identified through DHCP fingerprint detection. This field displays No Match for devices that do not match the filter criteria and those that do not have any DHCP fingerprint information. For information about DHCP fingerprints, see About DHCP Fingerprints.

**DHCPv4 Range Utilization Trend**

The **DHCPv4 Range Utilization Trend** dashboard provides DHCP usage trends for the top five most utilized address ranges in a given time frame. The default dashboard includes the top five most utilized DHCP ranges among all network views, all members, all subnets, and all IPv4 addresses.

The default dashboard displays line graphs for the top five most utilized address ranges and shows their DHCPv4 usage trends over the last 24 hours. Each of the five address ranges is represented with a different color line graph.

**DHCPv4 Usage Statistics**

The **DHCPv4 Usage Statistics** dashboard provides the overall DHCPv4 usage in a given time frame. The default dashboard includes all network views, all members, all subnets, all IPv4 addresses, and all DHCP ranges, and the default time frame is the last hour. The table is sorted by DHCP utilization rate.

This dashboard displays the following information in table format:

• **Timestamps**: The date and time of the event.

• **Network View**: Filter by a specific network view.

• **Network**: The network address.
CIDR: The subnet mask in CIDR format.

AD Site: The Active Directory Site associated with the network. For networks that are not associated with Active Directory Domains and Sites, or when you delete an Active Directory server, the appliance displays **no_value** in this column.

DHCPv4 Utilization: The percentage of DHCP address in use over the total number of DHCP addresses provisioned.

Ranges: The total number of IP address ranges in the network.

Provisioned: The total number of DHCP addresses configured.

Dynamic: The number of dynamic DHCP leases issued.

Static: The number of static DHCP addresses configured.

Free: The number of free DHCP addresses.

Used: The total number of DHCP addresses in use.

**DHCPv4 Usage Trend**

The **DHCPv4 Usage Trend** dashboard provides the overall DHCP usage trend for all members in a given time frame. The default dashboard includes information about all DHCP ranges in all network views, all members, all subnets, and all IPv4 addresses. It displays line graphs for the dynamic, static, and free DHCPv4 leases and shows their DHCPv4 usage trends over the last 24 hours. Each of the DHCPv4 leases is represented with a different color line graph.

This dashboard displays the following information:

- **Time**: The timestamp of the event.
- **Dynamic**: The number of dynamic DHCP leases issued.
- **Static**: The number of static DHCP addresses configured.
- **Free**: The number of free DHCP addresses.

Each of the line graphs is represented with a different color. When you select more than one member as the filter criteria, the dashboard displays line graphs for each of the following data: Dynamic, Static, and Free, for each selected member.

**Microsoft Servers**: Specify Microsoft servers assigned to networks and DHCP ranges. This filter is available even if no MS Management license installed on GM and Grid members.

**Top Device Classes**

The **Top Device Classes** dashboard lists the top DHCP fingerprint device class for requesting clients. The default dashboard displays the top 10 device classes along with the percentage of leased devices within the last 24 hours. The appliance lists the top detected device class in table format. You can click a specific row in the table to view all the devices in the class that belong to the selected device class. GUI displays the fingerprints that are detected under a selected device class. The total number of fingerprints of a specific device class is equal to the total number that is displayed against the corresponding device class.

This dashboard displays a table that contains the following information for each top DHCP fingerprint device class:

- **Device Class**: The device category or fingerprint class for the requesting clients.
- **Total**: The total number of leased clients that belong to this DHCP fingerprint class.
- **% of all devices**: The percentage of the leased clients belonging to this DHCP fingerprint class over the total number of requesting clients.

**Top Devices Denied an IP Address**

The **Top Devices Denied an IP Address** dashboard lists the top DHCP fingerprint devices used by remote clients that were denied a lease or an IP address based on the fingerprint filter criteria you specified. The default dashboard displays the top 10 devices per combination of fingerprint and network which were denied an IP address within the last 24 hours. For example, if the same device is denied from two separate networks during the past 24 hours, and/or with different fingerprints, then multiple events will be listed in the table corresponding to this device.

This dashboard displays a table that contains the following information for each denied DHCP fingerprint device class:

- **Mac/DUID**: The Mac address or DUID of the client's device.
- **Fingerprint**: The fingerprint description of the device used by remote clients.
- **Device Class**: The DHCP fingerprint class of the device used by remote clients.
- **Network**: The network to which the DHCP range belongs. For shared network, the network is the first network where the lease is prohibited due to fingerprint filter.
- **Attempts**: The total number of attempts by remote clients for an IP address in a given time frame.
- **Last Attempt**: The time stamp of the last attempt by remote client for an IP address in a given time frame.

**Top Devices Identified**

The **Top Devices Identified** dashboard lists the top DHCP fingerprints or detected operating systems for requesting clients. The appliance uses DHCP fingerprint detection to identify the operating systems or vendor IDs of remote clients. For more information about DHCP fingerprint detection, see **DHCP Fingerprint Detection**. The default dashboard displays the top 10 operating systems on which requesting clients are running within the last 24 hours.

The appliance lists the top detected operating systems or vendor IDs in table format. This dashboard shows the total number of different MAC devices that have requested a lease. You can click a specific row in the table to view a list of leased clients that belong to the selected operating
system or device type. Grid Manager displays another report that specifies more detailed information, such as the leased IPs and MAC addresses for each device that matches the selected DHCP fingerprint. The lease history for a fingerprint shows all the lease events that occurred during the time period specified with the parent search (Top Devices Identified report). It represents the number of devices that use the MAC/DUID as the unique identifier. Note that a single MAC address may have several lease events that occur within the specified time range for the parent search. Hence, the total number of each fingerprint will not be equal to the lease history of a fingerprint.

**Note:** You can use all available filters for the parent *Top Devices Identified* report, but you can filter the detailed report using only the *Fingerprint* column.

This dashboard displays a table that contains the following information for each top DHCP fingerprint:

- **Fingerprint:** The name of the DHCP fingerprint or vendor ID for the requesting clients.
- **Total:** The total number of leased clients that belong to this DHCP fingerprint.
- **% of all devices:** The percentage of the leased clients belonging to this DHCP fingerprint over the total number of requesting clients.

### DNS Dashboards

#### DDNS Update Rate Trend

The *DDNS Update Rate Trend* dashboard provides information about the dynamic DNS (DDNS) updates that occur on the DNS service. The default dashboard shows a line graph that tracks the rate of DDNS updates (counts per second) by query type in the given time frame. This dashboard displays DDNS updates per second by the following query type: Success, Failure, Reject, and Prerequisite Reject. The time is displayed according to the time zone specified on the reporting server in UTC format. You can mouse over the graph to display the coordinates of any point in the graph.

#### DNS Cache Hit Rate Trend

The *DNS Cache Hit Rate Trend* dashboard provides information about the cache hit ratio of selected Grid members. The dashboard shows line graphs that track cache hit rates over a given time frame. Note that if you have one member with two DNS views and requests are sent to only one DNS view, the maximum hit rate is 50% (not 100%) for the member because one DNS view has 100% hit rate and the other has 0, and the average is 50%.

**Note:** The *DNS Cache Hit Ratio Trend* is the search associated with the *DNS Cache Hit Rate Trend* report.

#### DNS Daily Peak Hour Query Rate by Member

The *DNS Daily Peak Hour Query Rate by Member* dashboard shows the average or peak DNS Query rate at the busiest hour within a day. This dashboard will help you identify the load that is being carried by each DNS Server during busy hours. This dashboard can help you plan better for capacity and reduce the risk of overloading DNS devices.

This dashboard displays the following information:

- **Time:** Timestamp of events.
- **QPS:** Query per second. QPS is calculated with two steps: 1) find out the busiest hour (on the top of hours such as from 8:00am to 9:00am) by average hourly QPS, and 2) use that hour's max/avg QPS as they daily max/avg QPS.

#### DNS Domain Query Trend

The *DNS Domain Query Trend* dashboard shows the trend of DNS queries for specific domains. This dashboard displays the DNS query trends for queries generated from both the internal and external sources.

#### DNS Domain Queried by Client

The *DNS Domain Queried by Client* dashboard shows the DNS domains being queried by the client. This dashboard displays the DNS domains that are being queried from both the internal and external sources.

#### Top DNS Clients by Query Type

The *Top DNS Clients by Query Type* dashboard lists the top DNS resource records that have been queried per client. This dashboard displays the DNS records query trends for queries that originate from both the internal and external sources.

#### Top DNS Clients Querying MX Records
The Top DNS Clients Querying MX Records dashboard lists the top MX records that have been queried per client. This dashboard displays the MX records query trends for queries that originate from both the internal and external sources.

DNS Daily Query Rate by Member

The DNS Daily Query Rate by Member dashboard shows the trend of the average or maximum daily DNS Query rate by member. This dashboard can help you identify the average or maximum daily load that is being carried by each DNS Server. This dashboard can help you plan better for capacity and reduce the risk of overloading DNS devices.

This dashboard displays the following information:

- **Time**: Timestamp of events.
- **QPS**: Query per second. QPS is calculated by the max/avg of 24 hourly QPS data per day (between midnights).

DNS Query Rate by Query Type

The DNS Query Rate by Query Type dashboard shows the trend of DNS queries per second by DNS record type. This dashboard displays line graphs of DNS query trends for selected DNS record types over a given time frame.

DNS Query Trend per IP Block Group

The DNS Query Trend per IP Block Group dashboard provides trend of DNS query counts aggregated over time intervals for user-defined IP block groups.

This dashboard displays the following information in table format:

- **Time**: Timestamp of events.
- **Group**: Name of the IP block group.
- **Query Count**: Total queries made to the IP block group for a specific time interval.

DNS Replies Trend

The DNS Replies Trend dashboard provides information about DNS query trends by message types. The dashboard shows line graphs that track DNS query replies by message type over a given time frame.

This dashboard displays line graphs of DNS query replies by the following query type: Failure, NXDomain, NXRRset, Referral, Success, Refused, and Other.

DNS Response Latency Trend

The DNS Response Latency Trend dashboard provides DNS latency response times for all or selected cache servers. This dashboard shows line graphs of DNS latency response times for each server.

DNS Effective Peak Usage Trend for Flex Grid License

The DNS Effective Peak Usage Trend for Flex Grid License dashboard lists the average of peak DNS queries per second for all IB-FLEX members in the Grid. The peak DNS queries per second are calculated as the maximum per day of average queries per second.

This dashboard displays the following information in either line chart or table format:

- **Show Filters**: Click Show Filters to enable the filters.
- **Time**: Select a value from the drop-down list. The default value is Last 30 days.
- **Line Chart**: Click Line Chart to view the data in line chart format.
- **Table**: Click Table to view the data in table format.
- **Both**: Click Both to view the data in both line chart and table format.

DNS Scavenged Object Count Trend

The DNS Scavenged Object Count Trend displays the number of removed stale DNS records per zone or DNS view over time. The default dashboard displays a reclaimed records count for the top five zones with the biggest number of records reclaimed over the last day.

DNS Query Rate by Member

The DNS Query Rate by Member dashboard shows the trend of DNS queries for selected members. This dashboard displays line graphs of DNS query trends for the selected members over a given time frame.
DNS Top Clients

The **DNS Top Clients dashboard** lists clients that have the most DNS queries. The dashboard shows horizontal bar charts that list clients that have the most total counts of DNS requests and their percentages over a given time frame. The default dashboard displays the top 10 clients within the last 24 hours. Note that the DNS Top Client report is not NAT client aware and therefore this dashboard does not show information for NATed clients.

To generate data for DNS Response Latency Trend dashboard, the Grid member enabled for DNS service queries itself for PTR record 1.0.0.127.in-addr.arpa every minute. NIOS will not exclude such DNS queries and displays default client 127.0.0.1 in the DNS Top Clients report.

DNS Top Clients Per Domain

The **DNS Top Clients Per Domain dashboard** lists the clients that have the most DNS queries for specified domain names and their subdomains. The dashboard shows a horizontal bar chart that lists the clients that have the most total counts of DNS requests and their percentages over a given time frame. You can display the report data in bar chart form or in table form. The domain or domains are specified using filters. The default dashboard displays the top 10 clients within the last 24 hours.

You can define the domains for capture in the Grid Reporting Properties editor (Administration tab -> Reporting tab -> Grid Reporting Properties -> DNS tab -> Monitor queries made to the following domains check box).

DNS Top NXDOMAIN / NOERROR (no data)

The **DNS Top NXDOMAIN / NOERROR (no data)** dashboard shows the number of responses transmitted by the specified name server(s) indicating a client-specified non-existent domain name. This dashboard displays horizontal bar graphs of DNS query trends for the selected members over a given time frame.

- NXDOMAIN indicates that no records of any type existed for the query name;
- NOERROR (no-data) indicates that no data existed for the requested resource record type; other records may exist for the query name.

**Note:** The statistical data on the IB-4030 appliance may not be absolutely accurate if acceleration cache entries are reused after the TTL expiration for other data during a given report monitoring interval. The default interval is 10 minutes.

DNS Top Requested Domain Names

The **DNS Top Requested Domain Names** dashboard lists the top most requested domain names, their counts and the percentage of request over a given time frame. The dashboard shows horizontal bar charts that list the total counts and request percentage for the top most requested domain names. The default dashboard displays the top 10 domain names within the last 24 hours.

**Note:** The statistical data on the IB-4030 appliance may not be absolutely accurate if acceleration cache entries are reused after the TTL expiration for other data during a given report monitoring interval. The default interval is 10 minutes.

DNS Top SERVFAIL Errors Sent

The **DNS Top SERVFAIL Errors Sent** dashboard lists the top query names resulting in Infoblox name servers sending DNS response packets containing the SERVFAIL message, to downstream clients. The length of the list of top queries, the time period for the report, and other parameters are specified using filters. The default dashboard displays the top 10 query names within the last 24 hours. When capturing queries, the Grid member matches authoritative and recursive queries to generate events for the report. This dashboard displays no DNS client information, or the identities of impacted name servers, when the SERVFAIL originates from an upstream server.

DNS Top SERVFAIL Errors Received

The **DNS Top SERVFAIL Errors Received** dashboard lists the top queries resulting in Infoblox name servers receiving DNS response packets containing the SERVFAIL message from upstream name servers. The length of the list of top queries, the time period for the report, and other parameters are specified using filters. The default dashboard displays the top upstream query names within the last 24 hours. (The upstream query name may be a query name supplied by a client, or another name that is needed while processing a client query.) When capturing queries, the Grid member matches recursive queries to generate events for the report. This dashboard displays no DNS client information, or the identities of impacted name servers. This dashboard reflects the exact numeric value of the number of queries.

DNS Top Timed-out Recursive Queries

The **DNS Top Timed-out Recursive Queries** dashboard shows the number of queries sent to Infoblox Grid member name servers, that result in timeouts after sending recursive queries to upstream name servers. This dashboard displays horizontal bar graphs of DNS query trends for the selected members over a given time frame.
DNS Traffic Control Resource Availability Status

The **DNS Traffic Control Resource Availability Status** dashboard provides the percentage of specific DNS Traffic Control resources that are available, partially available or unavailable over time. You can mouse over the pie chart to display the coordinates of any point in the pie chart. You can also drill down to view detailed data in table format.

This dashboard displays the following information:

- **Available**: Indicates if the resource is always available. When the availability of a resource is 100%, only then it is displayed as always available.
- **Partially Available**: Indicates if the resource is available sometimes. When the availability is less than 100% or more than 0%, only then it is displayed as partially available.
- **Unavailable**: Indicates if the resource is never available. When the availability is 0%, only then it is displayed as never available.

DNS Traffic Control Resource Availability Trend

The **DNS Traffic Control Resource Availability Trend** dashboard provides percentage of available DNS Traffic Control resources per server/health monitor pair over a period of time. You can aggregate data based on supported filtering categories and extensible attributes defined in the filtering feature.

The appliance aggregates data at every 10 minutes interval. You can mouse over the graph to display the coordinates of any point in the graph.

This dashboard displays the following information in either the line chart or table format:

- **Date and Time**: Timestamp of events.
- **Availability%**: Percentage of resources that are available.

DNS Traffic Control Resource Pool Availability Trend

The **DNS Traffic Control Resource Pool Availability Trend** dashboard provides information about the availability of load balanced resources that are grouped by extensible attributes over a selected period of time. The appliance aggregates data at every 10 minutes interval. You can mouse over the graph to display the coordinates of any point in the graph.

This dashboard displays the following information in either a line chart or a table format:

- **Time**: Timestamp of events.
- **Resource Pool**: The resource pools that are available.
- **Availability%**: The percentage of resource pools that are available.

DNS Traffic Control Resource Pool Availability Status

The **DNS Traffic Control Resource Pool Availability Status** dashboard provides information about the resource pools that are available, partially available, or unavailable at a certain time.

This dashboard displays the following information in a pie chart format:

- **Available**: Indicates if the resource pool is always available. When the availability of a resource pool is 100%, only then it is displayed as always available.
- **Partially Available**: Indicates if the resource pool is available sometimes. When the availability of a resource pool is less than 100% or more than 0%, only then it is displayed as partially available.
- **Unavailable**: Indicates if the resource pool is never available. When the availability of a resource pool is 0%, only then it is displayed as never available.

DNS Traffic Control Response Distribution Trend

The **DNS Traffic Control Response Distribution Trend** dashboard provides information about the number of responses returned by each resource. You can either group the results based on the resources in the pool, or by all resources with the associated same extensible attribute over a period of time. You can view how clients are load balanced or directed among different resources.

You can group the number of responses returned from each resource based on the pools. When you select **Resource Pool**, the appliance displays aggregated responses from resources belonging to a pool.

This dashboard displays the following information in either a line chart or a table format:

- **Time**: Timestamp of events.
- **Resource**: The resources that are available.
- **Responses**: The number of responses returned by each resource.

Security

**FireEye Alerts**
The FireEye Alerts dashboard lists the FireEye alerts that are received by the NIOS appliance. The dashboard displays the date and time when the alert was generated, mitigation action for the alert, ruleset specified for the blocked domain or IP address, and the name of the FireEye appliance that generated the alert. For more information about FireEye integrated RPZs, see Configuring FireEye RPZs.

Note: To enable this dashboard, you must select the Security check box in the Grid Reporting Properties editor. To select the check boxes, go to the Administration tab -> Reporting tab -> Grid Reporting Properties -> General tab -> Basic tab -> select the check box Security under Report Category. Note that you can receive this dashboard only on the Grid Master, not on Grid members, even if you have selected Security as a report category on the members.

This dashboard displays the following information in table format:

- **Time**: The date and time when the alert was generated.
- **AlertID**: The alert type along with the alert ID.
- **LogSeverity**: The severity of the alert, which can be Critical, Major, or Minor.
- **AlertType**: The type of alert received from the FireEye appliance.
- **FireEyeAppliance**: The FireEye appliance that generated the alert.
- **RPZEntry**: The RPZ rule specified for the FireEye alert.
- **MitigationAction**: The ruleset specified for the blocked domain name or IP address.

**DNS Top RPZ Hits**

The DNS Top RPZ Hits dashboard lists the top clients who received re-written responses through RPZ. The dashboard displays the total client hits and total rule hits over a given time frame. You can choose to view either the aggregated RPZ hits report or a detailed report of the top RPZ hits. In the Show filter, select Details to view the detailed report or select Aggregated Hits Count to view the aggregated report. When you select the Aggregated Hits Count option, the report data is consolidated based on the client ID, domain name, RPZ entry, RPZ severity, and mitigation action.

The appliance lists the top RPZ hits in table format. You can click a specific row in the table or the Client ID to view the DHCP lease history of a client. For information about DHCP lease history, see DHCP Lease History. Grid Manager displays another report that specifies more detailed information, such as the leased IPs, host name, and MAC addresses for each client. For more information about RPZs, see About Infoblox DNS Firewall. You can click Domain Name or RPZ Entry to view threat details of an RPZ rule. In addition, you can click the client IP address to view login details of the user. For information, see User History for IP Address.

You can compare the domain name and mitigation action in this dashboard with the RPZ rules and mitigation actions in the FireEye Alerts report to determine the RPZ hits received due to FireEye alerts.

Note: To enable this dashboard, you must select the DNS Query and Security check boxes in the Grid Reporting Properties editor. To select the check boxes, to the Administration tab -> Reporting tab -> Grid Reporting Properties -> General tab -> Basic tab -> select the check boxes DNS Query and Security under Report Category.

This dashboard displays the following information in table format:

- **Client ID**: The IP address of the client that queried the domain name that is listed in the RPZ ruleset.
- **Total Client Hits**: The total number of hits received for each DNS view from the respective client.
- **Domain Name**: The domain name that was queried.
- **Severity**: The threat severity level of an RPZ zone associated with the RPZ rule that was triggered.
- **RPZ Entry**: The RPZ rule that was triggered based on client queries.
- **Total Rule Hits**: The total number of hits received for a specific RPZ rule.
- **Mitigation Action**: The ruleset specified for the blocked domain name or IP address.
- **Substitute Addresses**: The address which was substituted for the blocked domain.
- **Time**: The date and time when the last hit was received. This information is displayed only in the detailed DNS Top RPZ Hits report.

The sub-dashboard Threat Details displays the following information in table format:

Note: Make sure that DNS resolution is enabled and running properly on the reporting member to view Threat Details.

- **RPZ Rule**: The RPZ rule that was triggered based on client queries.
- **First Identified**: The date and timestamp of the first occasion that the threat was detected.
- **Last Seen**: The date and timestamp of the last occasion that the threat was detected.
- **Threat Category**: The category to which the threat belongs.
- **Danger Level**: The severity level of the threat.
- **Short Description**: The brief description of an RPZ rule.
- **Description**: The detailed description of an RPZ rule.

**User History for IP Address**

The User History for IP Address sub-dashboard displays the login details of the active users associated with the IP address of the client. The default displays the following information in table format:

---

Copyright ©2019, Infoblox, Inc. All right reserved.
**User History for Lease IP**

You can view user information associated with the lease IP address. The default **User History for Lease IP** sub-dashboard displays the following information in table format:

- **Last Updated**: Displays the timestamp when the user information was last updated.
- **User Name**: The logon name of the user.
- **Domain**: The Active Directory domain name.
- **IP Address**: The IP address of the client.
- **First Seen**: The timestamp when the user logged in to the domain for the first time.
- **Logout Time**: The log out time of the user. This column displays NA when users are still active on the system.
- **Last Seen**: The timestamp when the user was last seen accessing a domain.
- **User Status**: Displays the status of the user. This can be one of the following: **Active** (logged in), **Logged Out**, **Timed Out**.
  - **Active**: The user is logged in and active.
  - **Logged Out**: The user has logged out of the system.
  - **Timed Out**: The user is logged in but has been idled for a certain period of time. The default is two hours. You can configure this time interval, as described in *Configuring Active User Timeout Session*.

**DNS Top RPZ Hits by Clients**

The **DNS Top RPZ Hits by Clients** dashboard lists the total number of RPZ hits from a client during an interval, irrespective of the rules and mitigation actions. You can view the IP address of the client, total hits and the date and time during which the hits were received.

The appliance lists the top RPZ hits by clients in table format. You can click a specific row in the table to view the lease history of a client. Grid Manager displays another report that specifies more detailed information, such as the leased IPs, host name, and MAC addresses for each client.

For more information about RPZs, see *About Infoblox DNS Firewall*. In addition, you can click the client IP address to view login details of the user. For information, see *User History for IP Address*.

This dashboard displays the following information in table format:

- **Client ID**: The IP address of the client that queried the domain name that is listed in the RPZ ruleset.
- **Total Client Hits**: The total number of hits received for all DNS view from the respective client.
- **Time**: The date and time when the last hit was received.

**Top DNS Firewall Hits**

The **Top DNS Firewall Hits** dashboard lists the top RPZ rules triggered over a given time frame. This dashboard lists information such as RPZ rule, percentage of RPZ rule hits, number of hits per RPZ rule, and the description of the threat that triggered the RPZ rule. The default dashboard displays the top 10 RPZ rules triggered within the last week.

*Note*: To enable this dashboard, you must select the DNS Query and Security check boxes in the Grid Reporting Properties editor. To select the check boxes, go to the Reporting tab -> Grid Reporting Properties -> General tab -> Basic tab, and then select the check boxes DNS Query and Security under Report Category.

The dashboard displays the following information in table format:

- **RPZ Rule**: The RPZ rule that was triggered based on client queries.
- **Percentage**: The percentage based on the number of hits for the RPZ rule divided by the total number of hits for the top RPZ rules.
- **# Hits**: The total number of hits received for the RPZ rule.
- **Description**: The detailed description of the threat that triggered the RPZ rule.

**DNS RPZ Hits Trend By Mitigation Action**

The **RPZ Hit Trend by Mitigation Action** dashboard provides trends for the total number of RPZ hits for each mitigation action along with the total client hits in a given time frame. You can view this report in either a line chart, a stacked chart, or in table format. You can choose to display the
The date and time when the last hit was received.

- **Time:** The date and time when the last hit was received.
- **Block:** Total number of queries that triggered a **Block (No Data)** and **Block (No Such Domain)** RPZ rule. For information about **Block (No Data)** and **Block (No Such Domain)** RPZ rules, see Managing Block (No Data) Rules and Managing Block (No Such Domain) Rules respectively.
- **Passthru:** Total number of queries that triggered the **Passthru** RPZ rule. For information about **Passthru** RPZ rule, see Managing Passthru Rules.
- **Substitute:** Total number of queries that triggered the **Substitute (Domain Name)** and **Substitute (Record)** RPZ rule. For information about **Substitute (Domain Name)** and **Substitute (Record)** RPZ rules, see Managing Substitute (Domain Name) Rules and Managing Substitute (Record) Rules respectively.
- **Client Hits:** Total number of queries that triggered an RPZ policy. The client hits is the sum of **Block (No Data)**, **Block (No Such Domain)**, **Passthru**, **Substitute (Domain Name)**, and **Substitute (Record)** RPZ hits. Note that this data is not displayed in the **Stacked Chart**, but displayed in the **Line Chart** and in **Table** format.

### Malicious Activity by Client

The **Malicious Activity By Client** dashboard lists the clients that have the most malicious activities. The default dashboard shows a bar chart that lists clients that have the most total counts of malicious activities that triggered the RPZ rule over the given time frame. The default dashboard displays the top 10 clients within the last week.

**Note:** To enable this dashboard, you must select the DNS Query and Security check boxes in the Grid Reporting Properties editor. To select the check boxes, go to the **Administration** tab -> Reporting tab -> Grid Reporting Properties -> General tab -> Basic tab, and then select the check boxes DNS Query and Security under Report Category.

This dashboard displays the following information:

- **Client ID:** The IP address of the client that queried the malicious domains.
- **# Hits:** The total number of RPZ hits by the client.
- **Domains:** The top three malicious domains queried by the client.
- **Last Active:** The timestamp of the last attempt when the client queried a malicious domain.

### DNS Firewall Executive Threat

The **DNS Firewall Executive Threat** dashboard is a predefined custom dashboard which consists of the following sub-dashboards:

- **Top DNS Firewall Hits**
- **Malicious Activity by Client**

**Note:** To enable this dashboard, you must select the DNS Query and Security check boxes in the Grid Reporting Properties editor. To select the check boxes, go to the **Administration** tab -> Reporting tab -> Grid Reporting Properties -> General tab -> Basic tab, and then select the check boxes DNS Query and Security under Report Category.

Note that you have to use the filters for each of the sub-reports to get specific information. You can also click **Download PDF** from the Toolbar to download the **DNS Firewall Executive Threat dashboard** in PDF format which includes the three-panel report in a single PDF.

### Threat Protection Event Count By Severity Trend

The **Threat Protection Event Count By Severity Trend** dashboard provides event count trends by severity in a given time frame. You can view event counts distributed for the following severity levels: Critical, Major, Warning and Informational. Each of the severity level of an event is represented with a different color.

You can also define alerts in this dashboard to notify administrators when a trend reaches a specified threshold. For information about how to define alerts, see **About IP Blocks and IP Block Groups**. When you configure alerts for this dashboard and define a threshold value to trigger SNMP traps for a specified reporting event type, the appliance triggers an alert every five minutes based on the filters you select. For information about how to trigger SNMP traps for reporting event types, see **Defining Thresholds for Traps**.

### Threat Protection Event Count By Member Trend

The **Threat Protection Event Count By Member Trend** dashboard provides event count trends on members that supports Advanced DNS Protection in a given time frame. This dashboard tracks events on a member over a given time frame. The default dashboard displays line chart that show events trends over the last day on the selected member. The default dashboard displays the top 5 appliances in descending order.
Threat Protection Event Count By Rule

The Threat Protection Event Count By Rule dashboard displays event counts based on violations of individual rules. The appliance displays event count by rule in table format and sorts the records by Total Event Count in descending order. You can click a specific Security ID in the table to view sub-report for the individual rule, showing aggregate event instances with timestamps for a specific rule on all members.

This dashboard displays the following information in table format:

- **SID**: The unique rule ID.
- **Category**: The category to which the rule belongs.
- **Log Severity**: The severity of an event, which can be **Critical**, **Major**, **Warning**, or **Informational**.
- **Event Name**: The name and description of the rule.
- **Alert Count**: The alert count of an event.
- **Drop Count**: The drop count of an event.
- **Total Event Count**: The total number of event counts triggered by a match against the rule.

The sub-dashboard Threat Protection Event Count for Rule displays the following information in table format:

**Note**: The sub-report Threat Protection Event Count for Rule displays all the detected events for a specific SID on all members, regardless of the filters you apply to the parent Threat Protection Event Count By Rule report.

- **Time**: The timestamp of an event.
- **SID**: The unique rule ID.
- **Member**: The name of the member that supports threat protection.
- **Category**: The category to which the rule belongs.
- **Log Severity**: The severity of an event, which can be **Critical**, **Major**, **Warning**, or **Informational**.
- **Event Name**: The name of a rule.
- **Alert Count**: The alert count of an event.
- **Drop Count**: The drop count of an event.
- **Total Event Count**: The total number of event counts triggered by a match against the rule.

Threat Protection Event Count By Time

The Threat Protection Event Count By Time dashboard displays event counts with timestamp in table format. This dashboard help you track security events behavior based on time of occurrence. For example, this dashboard indicates whether security events peak at specific times or if it has steadily increase over time.

This dashboard displays the following information in table format:

- **Time**: The timestamp of an event.
- **SID**: The unique rule ID.
- **Member**: The name of the member that supports threat protection.
- **Category**: The category to which the rule belongs.
- **Log Severity**: The severity of an event, which can be **Critical**, **Major**, **Warning**, or **Informational**.
- **Event Name**: The name and description of the rule.
- **Alert Count**: The alert count of an event.
- **Drop Count**: The drop count of an event.
- **Total Event Count**: The total number of event counts of a rule.

Threat Protection Event Count By Category

The Threat Protection Event Count By Category dashboard provides event counts by rule category. You can track rule categories that are under the most pressure from adverse events. This dashboard displays event counts in table format.

This dashboard displays the following information in table format:

- **Category**: The category to which a rule belongs.
- **Critical Event Count**: The number of critical events in the selected rule category.
- **Major Event Count**: The number of major events.
- **Warning Event Count**: The number of warning events.
- **Informational Event Count**: The number of informational events.
- **Total Event Count**: The total number of event counts triggered against a rule category.

Threat Protection Event Count By Member

The Threat Protection Event Count By Member dashboard provides event counts aggregated over time intervals for each member. This dashboard displays event count for each member in table format and sorts the records by Total Event Count in descending order.

This dashboard displays the following information in table format:

- **Member**: The name of the member that supports threat protection.
- **Critical Event Count**: The number of critical events on a member.
- **Major Event Count**: The number of major events detected on a member.
• **Warning Event Count:** The number of warning events detected on a member.
• **Informational Event Count:** The number of informational events detected on a member.
• **Total Event Count:** The total number of event counts detected on a member.

**Threat Protection Top Rules Logged**

The *Threat Protection Top Rules Logged* dashboard provides the list of the top 10 threat protection rules that are triggered by a source IP in a given time frame. You can also view the threat protection rules triggered by NAT'ed clients in a given time frame. You can view the source IP address, total number of events, rule name, and timestamp of the last event. If a rule is triggered by a NAT'ed client, then you can view the source IP address along with the port block of the NAT'ed client. You can also configure the appliance to display the report data in bar chart or in table form. The default dashboard displays bar chart for the top 10 rules that are triggered within the last seven days. This dashboard allows you to identify the IP address of a client and the rules it triggered.

**Note:** You can configure the top number of source IP addresses and threat protection rules on the appliance. For information about how to configure threat protection data, see *Configuring Threat Protection Data* on page 157.

This dashboard displays the following information in table format:

- **Rule:** The name and description of a rule that is triggered by the source IP. For each threat protection rule, the active count is displayed for the top three source IP addresses.
- **Logged Event Count:** The total number of events triggered against the rule.
- **Top Sources:** The IP address of the top sources triggering this rule. By default, the top 3 source IPs are displayed.
- **Last Active:** The timestamp when the rule was last active.

**Threat Protection Top Rules Logged by Source**

The *Threat Protection Top Rules Logged by Source* dashboard provides statistics about the total number of events triggered by the top sources (by client IP addresses) in a given time frame. You can also view the statistics for the total number of events triggered by NAT'ed clients in a given time frame. For example, if you configure a range of ports for a NAT'ed client, and if there are events logged from different port blocks of the NAT'ed client, then each port block is considered as a logical client in the dashboard. You can view the source IP address, total number of events, rule name, and timestamp of an event. If an event is triggered by a NAT'ed client, then you can view the source IP address along with the port block of the NAT'ed client. The default dashboard displays a bar chart for the top 10 source IPs that triggered threat protection rules within the last seven days. This dashboard allows you to identify the IP address of the client and the rules it triggered.

**Note:** You can configure the top number of source IP addresses and threat protection rules on the appliance. For information about how to configure threat protection data, see *Configuring Threat Protection Data*.

This dashboard displays the following information in table format:

- **Source:** The IP address of a source that triggered a threat protection rule.
- **Logged Event Count:** The total number of events triggered by a source against the rule.
- **Top Rules:** The name of the top rules triggered by each source IP. By default, the top three rules are displayed.
- **Last Active:** The timestamp when the source was last active.

**DNS Top Tunneling Activity**

The *DNS Top Tunneling Activity* dashboard lists the clients that have the most number of DNS tunneling activities in a given time frame. The default dashboard shows a horizontal bar chart that lists clients that have the most total counts of DNS tunneling events and their percentages over the given time frame. You can also configure the appliance to display this dashboard in table format. The default dashboard displays the top 10 clients within the last week. You can click the client IP address in the table or click the bar in the bar chart to view a sub-report *Rule hits for Client IP* for a specific client.

This dashboard displays the following information:

- **Client IP:** The source IP address that triggered the DNS tunneling event.
- **Event Count:** The total number of DNS tunneling events triggered by the client.

The sub-dashboard *Rule hits for Client IP* lists the number of events triggered by the selected client for each DNS tunneling category. It displays the following information in table format:

- **Category:** The category to which the DNS tunneling activity belongs. Category can include the type of DNS tunneling activities as well as tunneling tools used to generate the activities. A category can be *short TTL*, *NXDomain*, *high-entropy domains*, *Iodine tool*, and others.
- **Event Count:** The number of events triggered in each DNS tunneling category.
- **Last Seen:** The timestamp when the client was last active.

**DNS Tunneling Traffic by Category**
The **DNS Tunneling Traffic by Category** dashboard provides information about DNS tunneling activities by specific categories and the percentage of events by the category of DNS tunneling events in a given time frame. This dashboard helps you track abnormal DNS traffic. The default dashboard shows a pie chart that lists the categories of DNS tunneling events. You can mouse over the pie in the chart to view the DNS tunneling category, event counts, and their percentages. You can also configure the appliance to display this dashboard in table format. The default dashboard displays the top 10 DNS tunneling categories within the last week. You can click the category in the table or in the pie chart to view the sub-dashboard **DNS Top Tunneling Activity** dashboard for the selected category. For more information, see **DNS Top Tunneling Activity**. This dashboard displays the following information in table format:

- **Category**: The percentage based on the number of events in each DNS tunneling category divided by the total number of events in all the DNS tunneling categories.
- **Description**: The description about the rule that was triggered based on the client queries.

The sub-dashboard **DNS Top Tunneling Activity** dashboard displays the following information in table format:

- **Client IP**: The IP address of the client that triggered the DNS tunneling event.
- **Rule SID**: This field displays the rule ID for ADP rule hits. If you select **Detected by Analytics Engine** as the category, this field displays the name of the RPZ used for blacklisted domains detected through the analytics service.
- **Total DNS Tunneling Events**: The total number of DNS tunneling events triggered by the respective client.
- **Total Outbound malicious queries**: The total number of RPZ hits received from the respective client.
- **Last Seen**: The timestamp when the client was last active.

### Top Malware and DNS Tunneling Events by Client

The **Top Malware and DNS Tunneling Events by Client** dashboard lists the clients that have the most number of outbound malicious queries (RPZ hits) and DNS tunneling events in a given time frame. This dashboard lists the IP address of the client, total number of outbound malicious queries, total number of DNS tunneling events, and the timestamp when the client was last active. The appliance displays the report data in table format. You can click the client IP in the table to view the sub-report **Security Info for Client IP** for a specific client. This dashboard displays the following information in table format:

- **Client IP**: The IP address of the client that triggered the most number of outbound malicious queries (RPZ hits) and DNS tunneling events.
- **Total DNS Tunneling Events**: The total number of DNS tunneling events triggered by the respective client.
- **Total Outbound malicious queries**: The total number of RPZ hits received from the respective client.
- **Last Seen**: The timestamp when the client was last active.

The sub-dashboard **Security Info for Client IP** includes the DHCP and IP address management data along with the RPZ and DNS tunneling activities for the selected client. It displays the following information in table format:

- **Host Name**: The host name of the DHCP client.
- **MAC/DUID**: The MAC address or the DUID of the client.
- **Lease Start - Lease End**: The start and end date of the lease.
- **Fingerprint**: The DHCP fingerprint information of the client device.
- **Top 3 RPZ rules**: The top three RPZ rules triggered based on the queries from the selected client.
- **Top 3 DNS tunneling events**: The top three DNS tunneling events triggered by the selected client.
- **Device Name**: The name of the client device.
- **Port/Interface**: The name of the port or interface connected to the client device.

### Cloud Dashboard

#### VM Address History

The **VM Address History** dashboard provides VM address history in a given time frame. This dashboard is applicable only for the Cloud Network Automation solution. You can generate this dashboard to view activities over time for specific VM interfaces in the cloud environment. This dashboard lists information such as IP address, Action, MAC address, Port ID, FQDN, VM Name, Network, Tenant ID, and other fields associated with the VM interfaces. You can click a specific row in the table to view the **DHCP Lease History** dashboard for the VM. Grid Manager displays the **DHCP Lease History** dashboard below the **VM Address History** dashboard.

### Ecosystem Dashboards

#### User Login History Report

The **User Login History** dashboard provides information about user login activities in a given time frame. You can use this dashboard to audit user logins. This dashboard allows you to identify the IP address of a client, domains used by a user to login, the number of active users, and the login...
activities of a user over a period of time. This dashboard displays the following information in table format:

- **Last Updated**: Displays the timestamp when the user information was last synchronized with the Microsoft server.
- **User Name**: The logon name of the user.
- **Domain**: The Active Directory domain name.
- **IP Address**: The IP address of the client.
- **First Seen**: The timestamp when the user logged in to the Active Directory domain for the first time.
- **Logout Time**: The log out time of the user. This column displays NA when users are active on the Microsoft server.
- **Last Seen**: The timestamp when the user was last seen accessing an Active Directory domain.
- **User Status**: Displays the status of the user. This can be one of the following: **Active** (logged in), **Logged Out**, **Timed Out**.
  - **Active**: The user is logged in and active.
  - **Logged Out**: The user has logged out of the system.
  - **Timed Out**: The user is logged in but has been idled for a certain period of time. The default is two hours. You can configure this time interval, as described in Configuring Active User Timeout Session.

**Subscription Data**

The Subscription Data dashboard displays the user and device identity captured by the Cisco ISE for the subscribed member. The default dashboard displays user name, domain name, VLAN ID, Device operating system, and last discovered timestamp.

The predefined Subscription Data dashboard displays the following information:

- **User Name**: The logon name of the user.
- **Domain**: The domain name.
- **SSID**: Provision SSID. This is for corporate devices that connect to the corporate wireless SSID.
- **VLAN Name**: The name of the VLAN of the switch port.
- **VLAN ID**: The ID of the VLAN of the switch port.
- **Device OS**: Operating system of the device.
- **Session State**: The current status of the device.
- **Security Group**: Unique security group tag.
- **Discovered At**: Timestamp when the device was discovered.
- **Quarantine Status**: Indicates if the device should be quarantined or not.
- **IP Address**: The IP address of the client.
- **Grid ID**: The IP address of the subscribed member.

**Publish Data**

The Publish Data dashboard displays the RPZ, Security ADP, IPAM and DHCP lease information that is shared with the Cisco ISE. The default Publish Data dashboard displays the following information:

- **Last Updated**: Timestamp when the data was last updated for the device.
- **IP Address**: The source IP address that is publishing the data.
- **Target Address**: The IP address of the target Cisco ISE.
- **Publish Type**: The event type that is published.
- **Contents**: Additional details of the published information.

**System Utilization Dashboards**

**CPU Utilization Trend**

The CPU Utilization Trend dashboard provides CPU usage trends over a given time frame. The default dashboard displays line graphs that show CPU usage trends for up to five members in the Grid over the last 24 hours. Each of the members is represented with a different color line graph.

**Memory Utilization Trend**

The Memory Utilization Trend dashboard provides memory usage trends over a given time frame. The default dashboard displays line graphs that show memory usage trends for up to five members in the Grid over the last 24 hours. Each of the members is represented with a different color line graph.

**Traffic Rate by Member**

The Traffic Rate by Member dashboard provides inbound and outbound traffic over a given time frame. The dashboard displays line graphs that show traffic rate for members with reporting service enabled within the last 24 hours. Grid Manager uses different color line graphs to distinguish inbound and outbound traffic for different members.
Flex Grid Licensing Features Enabled

The Flex Grid Licensing Features Enabled dashboard lists the overall status of licensed features across all IB-FLEX members in the Grid. You can also view the status of each feature for individual members during a specified time period.

**Note:** When you move your mouse away from the FLEX Grid Licensing Features Enabled section, the Open in Search, Inspect, and Refresh icons might not show up in the GUI. You can view these icons when you move your mouse on the data displayed for the FLEX Grid Licensing Features Enabled dashboard.

This dashboard displays the following information in table format:

- **Feature:** Indicates the features on which the Flex Grid Activation license is installed.
  - **Active Trust Plus:** Displays Active Trust Plus as enabled on a member when any of the following RPZ feed zones are configured: antimalware-ip.rpz.infoblox.local, bot-ip.rpz.infoblox.local, exploitkit-ip.rpz.infoblox.local, malware-dga.rpz.infoblox.local, tor-exit-node-ip.rpz.infoblox.local, multi-domain.surbl.rpz.infoblox.local, and fresh-domain.surbl.rpz.infoblox.local.
  - **Active Trust Standard:** Displays Active Trust Standard as enabled on a member when any of the following RPZ feed zones are configured: base.rpz.infoblox.local, antimalware.rpz.infoblox.local, ransomware.rpz.infoblox.local, and bogon.rpz.infoblox.local.

**Note:** Active Trust Standard supports four zones whereas Active Trust Plus or Active Trust Advanced supports four zones and additional seven zones. This report displays the highest level of Active Trust support that is configured for a member.

- **Authoritative DNS:** Displays if DNS is enabled and authoritative zone is assigned to the member.
- **DNS Cache Acceleration:** Displays if DNS Cache Acceleration service is enabled on a member.
- **DNS Traffic Control:** Displays if DNS is enabled with resolver set to DNS server and the LBDN pool is configured for DNS Traffic Control.
- **FireEye:** Displays if DNS is enabled and FireEye zone is configured on a member.
- **Recursive DNS:** Displays information about whether DNS and recursion are enabled at the following levels:
  - Recursion is enabled at the member level.
  - Recursion is enabled at the Grid level and member inherits the setting.
  - Recursion is enabled for any DNS view assigned to a member.
- **Security Ecosystem:** Displays if TAXII is enabled on a member.
- **Threat Analytics:** Displays if Threat Analytics is enabled on a member.
- **Threat Protection:** Displays if Threat Protection service is enabled on a member.

License Pool Utilization

The License Pool Utilization dashboard provides information about the utilization of the dynamic licenses in a given time frame. This dashboard displays the total number of dynamic licenses available, percentage of pooled license allocation over time and other related information for each license pool. You can display the report data in table format, in line graph format, or both. Each of the line graphs, represented with a different color, is the utilization of licenses in one particular pool. The default dashboard displays the license pool utilization data for all the license pools. However, you can view the license pool utilization data for a specific license pool.

The default dashboard displays the following information:

- **Period/Date:** The time span of the license pool utilization.
- **License Pool:** The license pool such as vNIOS, DNS, DHCP, Grid, Cloud Platform, vNIOS CP-V800, and so on.
- **Total License Count:** The total number of available licenses.
- **Utilization (%):** The percentage of license pool utilization.

**Note:** The member details are not updated for alert emails in the Traffic Rate by Member report if the rises-by/drops-by operator is used. However, the member details are updated if you use the operators like greater than/less than in the alert filter.

System Capacity Prediction Trend

The System Capacity Prediction Trend dashboard forecasts the date and timestamp when the system resources such as CPU, database objects, DHCP leases, DNS queries meet its thresholds based on the current usage trends for the selected Grid member. This dashboard helps you determine the current usage, thresholds, and the predicted utilization over time. Using this dashboard, you can avoid unexpected usage of resources in your environment. In addition, you can scale the functional capacity for different appliance models.

The default dashboard displays the following information:

- **CPU Threshold**
  - **Max CPU Utilization:** Displays the maximum CPU used by the selected member.
  - **CPU Threshold Prediction:** Displays the predicted date and time when the CPU usage might reach its threshold based on your current usage.
  - **CPU Trend Prediction:** Displays the line graph to show the actual, threshold, and predicted CPU usage with a different color for the selected member and model type.
• **DB Objects Threshold**
  - **Max DB Objects Utilization**: The maximum number of database objects that is in use for the selected member.
  - **DB Objects Threshold Prediction**: Displays the predicted date and time when the database objects reach its thresholds based on your current usage trend.
  - **DB Objects Trend Prediction**: Displays the line graphs with different colors to show the actual database objects usage, database threshold value, and predicted database objects usage.

• **DNS Thresholds**
  - **Datasheet Max QPS**: The maximum number of queries sent to the selected member.
  - **QPS Threshold Prediction**: Displays the predicted date and time when the queries might reach its threshold based on your current trend.
  - **QPS Prediction**: Displays line graphs to show the actual number of queries, threshold, and predicted number of queries with a different color for the selected member.

• **DHCP Thresholds**
  - **Datasheet Max LPS**: Displays the appliance model and the number of DHCP leases issued.
  - **LPS Threshold Prediction**: Displays the predicted date and time when the DHCP leases might reach its threshold based on your current usage trend.
  - **DHCP Activity Prediction**: Displays the line graphs with a different color to show the actual, threshold, and predicted count of DHCP leases.

**IPAM Prediction Dashboard**

The IPAM Prediction dashboard provides information about the subnet utilization and DHCPv4 utilization in a graphical form to track the address usage trends over a time frame. This dashboard predicts the number of addresses used, configured thresholds for IPAM utilization, and forecasts the estimated address usage based on the current usage trends. Each of the line graphs is represented with a different color.

**Internal Reports**

You can monitor information about index volume usage on the reporting server for each report category and reporting members. You can track volume usage statistics by generating the following internal reports:

- Reporting Index Usage Statistics
- Reporting Volume Usage Trend per Category
- Reporting Volume Usage Trend per Member

**Reporting Index Usage Statistics**

The Reporting Index Usage Statistics dashboard provides information about the current disk space in use and the maximum index space configured for a reporting index. For information about the maximum index size allocated for each index, see Table 40.8. The dashboard shows a bar chart for Index Disk Usage trend. You can mouse over the bar to view the index volume usage/maximum index space allocated for that reporting index.

**Note**: The Reporting Index Usage Statistics dashboard displays information for only those indexes that demonstrate activities or disk usage. So even if the indexes are enabled but have no activity or disk usage, then information about these indexes is not displayed in the Reporting Index Usage Statistics dashboard.

This dashboard shows the following information:

- **Index (Reporting Member)**: The name of the index that holds specific types of reporting data.
- **Index Disk Usage Trend (% used/day)**: The percentage of index disk usage on a daily basis. The trend shows the impact of changing the reporting partition disk allocation and index capacities.
- **Earliest Event**: The timestamp of the earliest event in the index.
- **Max Volume (MB)**: The maximum index volume configured.
- **Usage (%)**: The percentage of disk space that is currently in use for the index.
- **Volume (MB)**: The current index volume in use.

**Reporting License Usage**

The Reporting License Usage dashboard provides license usage over a given time frame and license usage warning count if there is any license usage violation. The default dashboard displays bar chart that shows license usage in megabytes over a given time frame. This dashboard shows the following information:

- **License Usage (MB)**: The total reporting volume used by each report category in megabytes.
- **Time**: The timestamp of license usage.
- **License Usage Warning Count**: The warning count triggered due to license usage violation.
Reporting Volume Usage Trend per Category

The Reporting Volume Usage Trend per Category dashboard provides reporting volume usage trends over a given time frame. The default dashboard displays line chart that show reporting volume usage trends for report categories over the last day. This dashboard shows the following information:

- **Volume (MB):** The total reporting volume used by each report category in megabytes.
- **Time:** The timestamp of events.

Reporting Volume Usage Trend per Member

The Reporting Volume Usage Trend per Member dashboard provides reporting volume usage trends on members in a given time frame. The default dashboard shows line graphs that track reporting volume usage trends on a member within the last day. This dashboard shows the following information:

- **Volume (MB):** The total reporting volume used by each reporting member in megabytes.
- **Time (UTC):** The timestamp of events.

Managing Reporting Data

You can do the following to manage the Reporting and Analytics App:

- Upgrade Reporting and Analytics App, as described in Upgrading Reporting and Analytics App.
- Back up the reporting data, as described in Backing Up Reporting Data.
- Schedule the backup of the Reporting and Analytics App, as described in Scheduling the Backup of the Reporting Database.
- Restore the Reporting and Analytics App, as described in Restoring the Reporting Database.

Upgrading Reporting and Analytics App

You can download the latest version of the Infoblox Reporting and Analytics App from the Infoblox Support site. You can then upgrade this App on your reporting server.

To upgrade the Reporting and Analytics App:

1. Check your current version of the App in the Reporting Help tab.
2. Check if there is a later version that is available on the Infoblox Support site.
3. Download the .bin2 file from Infoblox Support site.
4. From the Administration tab, select the Reporting tab.
5. Click Upgrade Reporting & Analytics App from the Toolbar.
6. In the Upgrade Reporting & Analytics App dialog box, click Select. In the Upload dialog box, click Select, navigate to the .bin2 file, select it, and then click Upload.
7. After the Reporting and Analytics App is upgraded, click Restart to restart the Reporting service.

Backing Up and Restoring the Infoblox Reporting and Analytics App

To back up the Reporting and Analytics App, go to the Grid tab, select Backup -> Grid Backup -> Manual Backup from the Toolbar, and then select Infoblox Reporting & Analytics App to back up the app. When you back up the Reporting and Analytics App, the backup file is a .bak file that contains the reporting settings configured in the Grid Reporting Properties.

To restore the Reporting and Analytics App, go to the Grid tab, select Restore -> Restore Grid from the Toolbar, and then select Infoblox Reporting & Analytics App to restore the app.

Backing Up Reporting Data

Before you back up the reporting database, ensure that the reporting service is enabled on the reporting server. You cannot perform or schedule a backup if the reporting service is disabled on the reporting server. If you want to upgrade your reporting server, back up all the data. If you want to upgrade your reporting server, back up all the data before you power down the server. During an upgrade, the reporting server is automatically upgraded after the Grid Master. You cannot control or schedule when to upgrade the reporting server. For information about upgrades and upgrade groups, see Managing Upgrade Groups.

Note that reporting data backups are incremental backups, which means that backup files are copied to the designated file server only when there are new events generated since the last backup. Backing up of the reporting database to an FTP or SCP server using IPv4 or IPv6 is supported. The backup file is a .tar.gz file that contains the reporting data.

**Note:** If you stop an ongoing backup process, backup files are still being copied to the designated file server. When you perform a subsequent backup, the appliance appends incremental data to these backup files.

You can manually back up the reporting database or schedule a backup, but you cannot perform both at the same time. The backup process starts when the indexed data rolls from the hot bucket to the warm bucket. The hot bucket includes all inbound events and actively written data.
Indexed data moves to the warm bucket when one of the following conditions is met:

- The size of the reporting data reaches 1 GB
- Data is 90 days old
- The reporting server restarts

You can perform the following reporting data backups:

- Manual backups, as described in *Backing Up the Reporting Database Manually*.
- Scheduled backups, as described in *Scheduling the Backup of the Reporting Database*.

### Backing Up the Reporting Database Manually

1. From the **Grid** tab, select **Backup -> Reporting Backup -> Manual Backup** from the Toolbar.
2. In the **Manual Reporting Backup** editor, complete the following:
   - **Backup to**: Select the destination of the backup file from the drop-down list:
     - **FTP**: Back up the reporting database to an FTP server.
     - **Filepath**: Enter the directory path. For example, you can enter `/archive/backups/Infoblox/`
     - **IP Address of FTP Server**: The IP address of the FTP server.
     - **Username**: Enter the username of your FTP account.
     - **Password**: Enter the password of your FTP account.
     - **SCP**: Back up the reporting database to an SSH server that supports SCP.
     - **Filepath**: Enter the directory path. For example, you can enter `/archive/backups/Infoblox/`
     - **IP Address of SCP Server**: The IP address of the SCP server.
     - **Username**: Enter the username of your SCP account.
     - **Password**: Enter the password of your SCP account.

**Note**: When you select FTP or SCP, ensure that you have a valid username and password on the server prior to backing up the files.

### Scheduling the Backup of the Reporting Database

1. From the **Grid** tab, select **Backup -> Reporting Backup -> Schedule Backup** from the Toolbar.
2. In the **Schedule Reporting Backup** editor, complete the following:
   - **Status**: Displays the status of the backup process of the last operation. Select the destination of the backup file from the **Backup to drop-down list**:
     - **FTP**: Back up the reporting database files to an FTP server.
     - **Filepath**: Enter the directory path. For example, you can enter `/archive/backups/Infoblox/`
     - **IP Address of FTP Server**: The IP address of the FTP server.
     - **Username**: Enter the username of your FTP account.
     - **Password**: Enter the password of your FTP account.
     - **SCP**: Back up the reporting database to an SSH server that supports SCP.
     - **Filepath**: Enter the directory path. For example, you can enter `/archive/backups/Infoblox/`
     - **IP Address of SCP Server**: The IP address of the SCP server.
     - **Username**: Enter the username of your SCP account.
     - **Password**: Enter the password of your SCP account.

**Recurrence** Select how often you want to back up the files. You can select **Weekly**, **Daily**, or **Hourly** from the drop-down list. When you select **Weekly**, complete the following:
   - **Every**: Choose a day of the week from the drop-down list.
   - **Time**: Enter a time in the `hh:mm:ss AM/PM` format. You can also click the clock icon and select a time from the drop-down list. The Grid Master creates a backup file on the selected day and time every week.

When you select **Daily**, enter a time in the `hh:mm:ss AM/PM` format. You can also select a time from the drop-down list.

When you select **Hourly**, complete the following:
   - **Minutes after the Hour**: Enter the minute after the hour when the Grid Master creates a backup file. For example, enter 5 if you want the Grid Master to create a backup file five minutes after the hour every hour.
   - **Disable Scheduled Backup**: Select this if you want to disable automatic backups from occurring now, but want to save the settings for future use.

**Note**: When you select FTP or SCP, ensure that you have a valid username and password on the server prior to backing up the files.
Restoring the Reporting Database

Restoring the reporting database may take a long time to perform, and the reporting service is unavailable during a restore. Ensure that you must restore the reporting database before you perform the operation. Restoring of reporting database from an FTP or SCP server using IPv4 or IPv6 is supported.

Note the following during a restore:

- The reporting service is unavailable.
- Existing reporting data is removed from the reporting server.
- Backup data is restored up to the amount the reporting server can accommodate.

Note: The Volume Used Today displayed in the Device Information section will not be updated after restoring the data. Also, when you restore data or execute the CLI command reset reporting_data, the volume violation count will be reset to zero on the second day.

1. From the Grid tab, select Restore -> Restore Reporting from the Toolbar.
2. In the Restore dialog box, complete the following:
   - Status: Displays the status of the restore process, if in progress.
   - Select the destination of the backup file from the Restore from drop-down list:
     - FTP: Restore the reporting backup files from an FTP server.
       - Filepath: Enter the directory path. For example, you can enter /archive/backups/Infoblox/.
       - IP Address of FTP Server: The IP address of the FTP server.
       - Username: Enter the username of your FTP server account.
       - Password: Enter the password of your FTP server account.
     - SCP: Restore the reporting backup files from a SCP server.
       - Filepath: Enter the directory path. For example, you can enter /archive/backups/Infoblox/.
       - IP Address of SCP Server: The IP address of the SCP server.
       - Username: Enter the username of your SCP server account.
       - Password: Enter the password of your SCP server account.
3. Click Restore.

Infoblox-4030 Supported Dashboards

The IB-4030 appliance provides the following predefined dashboards:

DNS Reports
- DNS Replies Trend
- DNS Top Clients
- DNS Query Rate by Query Type
- DNS Response Latency Trend
- DNS Query Rate by Member
- DNS Replies Trend
- DNS Replies Trend
- DNS Top SERVFAIL Errors Sent
- DNS Top SERVFAIL ErrorsReceived
- DNS Top Timed-out RecursiveQueries
- DNS Top Requested DomainNames
- DNS Top Clients
- DNS Top NXDOMAIN /NOERROR (no data)

Security (DNS) Reports
- DNS Top RPZ Hits
- DNS Top RPZ Hits by Clients
- FireEye Alerts
- Threat Protection Event Count By Severity Trend
- Threat Protection Event Count By Rule
- Threat Protection Event Count By Time
- Threat Protection Event Count By Category
- Threat Protection Event Count By Member
- Threat Protection Event Count By Member Trend
- DNS Top Tunneling Activity
- DNS Tunneling Traffic by Category
- Top Malware and DNS Tunneling Events by Client

System Reports
• CPU Utilization Trend
• Memory Utilization Trend
• Traffic Rate by Member
• License Pool Utilization

Reports with Data Synchronized from Microsoft Servers

**Note:** The DNS reports listed in the following table displays data synchronized from the Microsoft servers only when you have enabled synchronization of reporting data for the Grid or the Microsoft servers. For information about enabling synchronization of DNS reporting data from the Microsoft server, see [Synchronizing DNS Reporting Data](#).

Infoblox supports the following versions of Microsoft Windows servers in displaying reporting data from both NIOS and the Microsoft servers:


The following reports display data from both NIOS and the Microsoft servers:

**DNS Reports**

- DNS Top Requested Domain Names
- DNS Top Clients
- DNS Top Clients Per Domain
- DNS Query Rate by Query Type
- DNS Query Rate by Member
- DNS Daily Query Rate by Member
- DNS Daily Peak Hour Query Rate by Member
- DNS Top NXDOMAIN/NOERROR (no data)
- DNS Top SERVFAIL Errors Sent
- DNS Top SERVFAIL Errors Received
- DNS Top Timed-out Recursive Queries
- DNS Query Trend per IP Block Group
- DDNS Update Rate Trend

Following DNS reports are generated if a Data Collector VM is registered with the Grid:

- DNS Domain Queried by Client
- DNS Domain Query Trend
- Top DNS Clients by Query Type
- Top DNS Clients Querying MX Records

**DHCP Reports**

- DHCPv4 Usage Trend
- DHCPv4 Usage Statistics
- DHCPv4 Range Utilization Trend
- DHCPv4 Top Utilized Networks
- DHCP Lease History
- DHCP Top Lease Clients
- DHCP Message Rate Trend

**IPAM Reports**

- IPAMv4 Network Usage Statistics
- IPAMv4 Network Usage Trend
- IPAMv4 Top Utilized Networks

## Chapter 41 Reporting Data Model

This section contains information about fields that are included in the reports and dashboards. You can find the commonly extracted fields and their specifications such as data source and range, which can help you better define your dashboards and searches.

**Splunk default fields**
Splunk server adds the following default fields to each event in every index.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Values/Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>date_hour</td>
<td>Indicates the hour when an event occurred. To narrow your search for specific event timestamps, you can use the default datetime fields. Click <a href="#">here</a> for more information on datetime fields.</td>
<td>Range: 0-23</td>
</tr>
<tr>
<td>date_mday</td>
<td>Indicates the day of the month when the event occurred</td>
<td>Range: 1-31</td>
</tr>
<tr>
<td>date_minute</td>
<td>Indicates the exact minute when the event occurred</td>
<td>Range: 0-59</td>
</tr>
<tr>
<td>date_month</td>
<td>Indicates the month during which an event occurred</td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Indicates the second in which an event occurred</td>
<td>Range: 0-59</td>
</tr>
<tr>
<td>date_wday</td>
<td>Indicates the day of the week in which an event occurred</td>
<td>Example: Sunday, Monday, etc.</td>
</tr>
<tr>
<td>date_year</td>
<td>Indicates the year in which an event occurred</td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Indicates the time for the local timezone of an event, expressed as hours in Unix Time</td>
<td></td>
</tr>
<tr>
<td>eventtype</td>
<td>Indicates events of the same type based on a given search. Click <a href="#">here</a> for more information.</td>
<td>Example: splunkd-log</td>
</tr>
<tr>
<td>host</td>
<td>Contains information about the originating hostname or a network IP address that generates the event</td>
<td>Example: reporting-1.com</td>
</tr>
<tr>
<td>index</td>
<td>Contains the name of the index with which a given event is indexed</td>
<td>Example: ib_dns_summary</td>
</tr>
<tr>
<td>linecount</td>
<td>Contains information about the number of lines in an event before it is indexed</td>
<td>Example: 1</td>
</tr>
<tr>
<td>punct</td>
<td>Contains information about the pattern of the first thirty punctuation characters in the first line of the event with which it is associated. It shows how an event looks when all letters, numbers, and spaces are removed and contains characters such as periods, colons, parentheses, quotes, question marks, dashes, and underscores. Click here for more information.</td>
<td>Example: -:[]_--=/</td>
</tr>
<tr>
<td>source</td>
<td>Contains the name of the file, stream, or other input details from which the event originates</td>
<td>Example: si-search-dns-query-reply</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Specifies the format of data input from which the event originates</td>
<td>Stash</td>
</tr>
<tr>
<td>splunk_server</td>
<td>Contains the name of the Splunk server that comprises the event</td>
<td>Example: reporting-2.com-2-slave</td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Contains the name of the Splunk server group</td>
<td>String</td>
</tr>
</tbody>
</table>

**Commonly extracted fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>date_hour</td>
<td>Indicates the hour when an event occurred. To narrow your search for specific event timestamps, you can use the default datetime fields. Click <a href="#">here</a> for more information on datetime fields.</td>
<td>Range: 0-23</td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Indicates the day of the month when the event occurred</td>
<td>Range: 1-31</td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Indicates the exact minute when the event occurred</td>
<td>Range: 0-59</td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Indicates the month during which an event occurred</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Indicates the second in which an event occurred</td>
<td>Range: 0-59</td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Indicates the day of the week in which an event occurred</td>
<td>Example: Sunday, Monday, etc.</td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Indicates the year in which an event occurred</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Indicates the time for the local timezone of an event, expressed as hours in Unix Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eventtype</td>
<td>Indicates events of the same type based on a given search. Click <a href="#">here</a> for more information.</td>
<td>Example: splunkd-log</td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>Contains information about the originating hostname or a network IP address that generates the event</td>
<td>Example: reporting-1.com</td>
<td></td>
</tr>
<tr>
<td>index</td>
<td>Contains the name of the index with which a given event is indexed</td>
<td>Example: ib_dns_summary</td>
<td></td>
</tr>
<tr>
<td>linecount</td>
<td>Contains information about the number of lines in an event before it is indexed</td>
<td>Example: 1</td>
<td></td>
</tr>
<tr>
<td>punct</td>
<td>Contains information about the pattern of the first thirty punctuation characters in the first line of the event with which it is associated. It shows how an event looks when all letters, numbers, and spaces are removed and contains characters such as periods, colons, parentheses, quotes, question marks, dashes, and underscores. Click here for more information.</td>
<td>Example: -:[]_--=/</td>
<td></td>
</tr>
<tr>
<td>source</td>
<td>Contains the name of the file, stream, or other input details from which the event originates</td>
<td>Example: si-search-dns-query-reply</td>
<td></td>
</tr>
<tr>
<td>sourcetype</td>
<td>Specifies the format of data input from which the event originates</td>
<td>Stash</td>
<td></td>
</tr>
<tr>
<td>splunk_server</td>
<td>Contains the name of the Splunk server that comprises the event</td>
<td>Example: reporting-2.com-2-slave</td>
<td></td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Contains the name of the Splunk server group</td>
<td>String</td>
<td></td>
</tr>
</tbody>
</table>
EA

Specifies the extensible attribute

String

| __grouping_by_ea_tag_lookup lookup from /storage/splunk/etc/apps/infoblox/lookups/grouping_by_ea_tag_map.csv with host value as input |
| pool_ea_lookup_csv lookup from /storage/splunk/etc/apps/infoblox/lookups/idns_pools.csv with pool value as input |
| resource_pool_ea_lookup_csv lookup from /storage/splunk/etc/apps/infoblox/lookups/idns_resources.csv with RESOURCE value as input |
| network_ea_lookup_csv lookup from /storage/splunk/etc/apps/infoblox/lookups/network.csv with NETWORK value as input |

HWTYPE

Specifies the hardware type

Example: IB-4030

| nios_member_hw_lookup lookup from /storage/splunk/etc/apps/infoblox/lookups/nios_member_hw.csv with host value as input |

MAX_DB_OBJECTS

Specifies the maximum objects in the database for a host

eg: 8000000

| nios_member_hw_lookup lookup from /storage/splunk/etc/apps/infoblox/lookups/nios_member_hw.csv with host value as input |

MAX_DHCP_LPS

Specifies the maximum number of DHCP leases per second for a host

Example: 15.0

| nios_member_hw_lookup lookup from /storage/splunk/etc/apps/infoblox/lookups/nios_member_hw.csv with host value as input |

MAX_DNS_QPS

Specifies the maximum DNS queries per second for a host

Example: 1000000.0

| nios_member_hw_lookup lookup from /storage/splunk/etc/apps/infoblox/lookups/nios_member_hw.csv with host value as input |

MEMBER_IP

Specifies the IP address of the member

IP address

| nios_member_hw_lookup lookup from /storage/splunk/etc/apps/infoblox/lookups/nios_member_hw.csv with host value as input |

timeendpos

 Specifies the byte at which the timestamp ends. These values are based on the TIME_FORMAT that is specified for a sourcetype under props.conf.

Example: 26


timestartpos

 Specifies the byte at which the timestamp starts

Example: 0

Indexes and Extracted Data

Infoblox Audit Logs

Most of the fields in this index are extracted directly from the audit.log file. Some of them are mentioned in the table below:

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTION</td>
<td>Indicates the action taken</td>
<td>String. Example: Called</td>
<td>Infoblox audit logs</td>
</tr>
<tr>
<td>ADMIN</td>
<td>Indicates the name of the admin</td>
<td>String. Example: root</td>
<td>Infoblox audit logs</td>
</tr>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXEC_STATUS</td>
<td>Indicates the execution status</td>
<td>String. Example: Pending Approval</td>
<td>Infoblox audit logs</td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td>MESSAGE</td>
<td>Indicates the message</td>
</tr>
<tr>
<td>OBJECT_NAME</td>
<td>Indicates the object name</td>
<td>OBJECT_TYPE</td>
<td>Indicates the object type</td>
</tr>
<tr>
<td>TIMESTAMP</td>
<td>Indicates the timestamp</td>
<td>action</td>
<td>Indicates the action</td>
</tr>
<tr>
<td>address</td>
<td>Example: 10.0.0.0</td>
<td>auth</td>
<td>Example: Local</td>
</tr>
<tr>
<td>cidr</td>
<td>Example: 8</td>
<td>code</td>
<td>Example: created</td>
</tr>
<tr>
<td>comment</td>
<td>String</td>
<td>date_hour</td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td>date_minute</td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td>date_second</td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td>date_year</td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td>eventtype</td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>group</td>
<td>Example: admin-group</td>
<td>host</td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td>linecount</td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>member</td>
<td>Example: Member:infoblox.localdomain</td>
<td>network_view</td>
<td>Example: default</td>
</tr>
<tr>
<td>punct</td>
<td>Splunk Default field</td>
<td>source</td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Splunk Default field</td>
<td>splunk_server</td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Splunk Default field</td>
<td>user</td>
<td>Example: admin</td>
</tr>
</tbody>
</table>

Infoblox DNS Query, DNS Performance, DDNS, DNS Record Scavenging

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLIENT</td>
<td>Indicates the DNS client</td>
<td>String</td>
<td>Infoblox DNS query</td>
</tr>
<tr>
<td>COUNT</td>
<td>Indicates the count</td>
<td>Integer</td>
<td>Infoblox DNS query and DNS Record Scavenging</td>
</tr>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Type</td>
<td>Source</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------</td>
<td>------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>FQDN</td>
<td>Indicates the FQDN</td>
<td>String</td>
<td>Infoblox DNS query</td>
</tr>
<tr>
<td>HITS</td>
<td>Indicates the DNS cache hits count</td>
<td>Integer</td>
<td>Infoblox DNS query</td>
</tr>
<tr>
<td>HNAME</td>
<td>Indicates the HNAME</td>
<td>String</td>
<td>Infoblox DNS query</td>
</tr>
<tr>
<td>HWTYPE</td>
<td><strong>Common Extracted fields</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LATENCY</td>
<td>Indicates the latency count</td>
<td>Integer</td>
<td>Infoblox DNS performance</td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td><strong>Common Extracted fields</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td><strong>Common Extracted fields</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td><strong>Common Extracted fields</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER</td>
<td>Specifies the member</td>
<td>String</td>
<td>DNS Record Scavenging</td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td><strong>Common Extracted fields</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MISSES</td>
<td>Specifies DNS cache miss count</td>
<td>Integer</td>
<td>Infoblox DNS query</td>
</tr>
<tr>
<td>QCOUNT</td>
<td>Specifies query count</td>
<td>Integer</td>
<td>Infoblox DNS query</td>
</tr>
<tr>
<td>REST</td>
<td>REST</td>
<td>String</td>
<td>Infoblox DDNS</td>
</tr>
<tr>
<td>SOURCE</td>
<td>SOURCE</td>
<td>String</td>
<td>Infoblox DDNS</td>
</tr>
<tr>
<td>SOURCEA</td>
<td>SOURCEA IP address</td>
<td>IP address</td>
<td>Infoblox DDNS</td>
</tr>
<tr>
<td>TLD</td>
<td>Specifies the top-level domain name</td>
<td>String</td>
<td>Infoblox DNS query</td>
</tr>
<tr>
<td>TYPE</td>
<td>RR Type</td>
<td>String</td>
<td>Infoblox DNS query and DNS Record Scavenging</td>
</tr>
<tr>
<td>TYPEA</td>
<td>TYPEA</td>
<td>String</td>
<td>Infoblox DDNS</td>
</tr>
<tr>
<td>VIEW</td>
<td>It refers to the DNS view key to map DNS view through lookup. See <code>display_name</code> field.</td>
<td>String</td>
<td>Infoblox DNS query</td>
</tr>
<tr>
<td>ZONE</td>
<td>Indicates the name of the zone</td>
<td>String</td>
<td>Infoblox DDNS</td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>display_name</td>
<td>Specifies the name of the DNS view</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>failure</td>
<td>Specifies the DNS FAILURE query count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nxdomain</td>
<td>Specifies the DNS NXDOMAIN query count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>nxrrset</td>
<td>Specifies the DNS NXRRSET query count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>other</td>
<td>Specifies the DNS other query count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>punct</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>referral</td>
<td>Specifies the DNS REFERRAL query count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>source</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sourcetype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>success</td>
<td>Specifies the DNS success query count</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeendpos</td>
<td>Common extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timestartpos</td>
<td>Common extracted fields</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Infoblox DNS Query Capture**

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>answer_count</td>
<td>Specifies the answer count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>display_name</td>
<td>Specifies the DNS view</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DNS view lookup from dns_viewkey_displayname.csv using View field value.</td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>flag_aa</td>
<td>Flag AA</td>
<td>Boolean. Example: Y</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>flag_ad</td>
<td>Flag AD</td>
<td>Boolean. Example: Y</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>flag_edns</td>
<td>Flag EDNS</td>
<td>Boolean. Example: Y</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>flag_recursion</td>
<td>Flag Recursion</td>
<td>Boolean. Example: Y</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>host_class</td>
<td>Specifies the host class</td>
<td>Example: IN</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>host_type</td>
<td>Specifies the host type</td>
<td>Example: PTR</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>message_type</td>
<td>Specifies the message type</td>
<td>Example: Query or Response</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>name</td>
<td>Specifies the name</td>
<td>Host name. Example: 1.0.0.127.in-addr.arpa</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>query</td>
<td>Specifies the query</td>
<td>Host name. Example: 213.31.102.10.in-addr.arpa</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>query_class</td>
<td>Specifies the query class</td>
<td>Example: IN</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>query_count</td>
<td>Specifies the query count</td>
<td>Integer. Example: 1</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>query_source</td>
<td>Specifies the query source</td>
<td>Example: I, E</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>query_type</td>
<td>Specifies the DNS query type</td>
<td>Example: PTR</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Values/Range</td>
<td>Source of Data</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td>rdata</td>
<td>RDATA</td>
<td>String. This value depends on the query type.</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>reply_code</td>
<td>Specifies the reply code</td>
<td>String. Example: ServFail, NoError</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>source</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sourcetype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>src_ip</td>
<td>Specifies the source IP</td>
<td>IP Address</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>src_port</td>
<td>Specifies the source port</td>
<td>Integer</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>time_msec</td>
<td>Specifies time in milliseconds</td>
<td>Integer</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>timeendpos</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timestamp</td>
<td>Indicates the timestamp</td>
<td>Integer</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>timestartpos</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>transport</td>
<td>Specifies the mode of transport</td>
<td>Example: UDP, TCP</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>ttl</td>
<td>Specifies the TTL</td>
<td>Integer. Example: 3600</td>
<td>Infoblox DNS query capture</td>
</tr>
<tr>
<td>view</td>
<td>Specifies the view</td>
<td>Example: 1, 2</td>
<td>Infoblox DNS query capture</td>
</tr>
</tbody>
</table>

**Infoblox DHCP Performance**

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK</td>
<td>Specifies the network address</td>
<td>Example: 10.0.0.0/8</td>
<td>Evaluated from address and cidr field values</td>
</tr>
<tr>
<td>address</td>
<td>Specifies the DHCP client address</td>
<td>IP address</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>address_total</td>
<td>Specifies the total number of addresses</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>cidr</td>
<td>Specifies the CIDR</td>
<td>Example: 24</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dhcp_hosts</td>
<td>Specifies the DHCP hosts count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcp_utilization</td>
<td>Specifies the DHCP utilization</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcp_utilization_status</td>
<td>Specifies the DHCP utilization status</td>
<td>String</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv4ack</td>
<td>Specifies the DHCPv4 ACK message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td>Type</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------</td>
<td>----------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>dhcpv4decline</td>
<td>Specifies the DHCPv4 decline message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv4discover</td>
<td>Specifies the DHCPv4 discover message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv4inform</td>
<td>Specifies the DHCPv4 inform message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv4leaseactive</td>
<td>Specifies the DHCPv4 lease active message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv4leasequery</td>
<td>Specifies the DHCPv4 lease query message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv4leaseunassigned</td>
<td>Specifies the DHCPv4 lease unassigned message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv4leaseunknown</td>
<td>Specifies the DHCPv4 lease unknown message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv4nak</td>
<td>Specifies the DHCPv4 NAK message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv4offer</td>
<td>Specifies the DHCPv4 offer message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv4release</td>
<td>Specifies the DHCPv4 release message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv4request</td>
<td>Specifies the DHCPv4 request message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6advertise</td>
<td>Specifies the DHCPv6 advertise message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6confirm</td>
<td>Specifies the DHCPv6 confirm message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6decline</td>
<td>Specifies the DHCPv6 decline message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6information_request</td>
<td>Specifies the DHCPv6 information request message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6leasequery</td>
<td>Specifies the DHCPv6 lease query message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6leasequery_reply</td>
<td>Specifies the DHCPv6 lease query reply message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6rebind</td>
<td>Specifies the DHCPv6 rebind message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6reconfigure</td>
<td>Specifies the DHCPv6 reconfigure message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6relay_forward</td>
<td>Specifies the DHCPv6 relay forward message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6relay_reply</td>
<td>Specifies the DHCPv6 relay reply message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6release</td>
<td>Specifies the DHCPv6 release message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6renew</td>
<td>Specifies the DHCPv6 renew message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6reply</td>
<td>Specifies the DHCPv6 reply message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6request</td>
<td>Specifies the DHCPv6 request message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>dhcpv6solicit</td>
<td>Specifies the DHCPv6 solicit message count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>display_name</td>
<td>Specifies the DNS View</td>
<td>String</td>
<td>DNS view lookup from dns_viewkey disp layname.csv using View field value</td>
</tr>
<tr>
<td>dynamic_hosts</td>
<td>Specifies the dynamic hosts count</td>
<td>Integer</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>end_address</td>
<td>Specifies the end IP address</td>
<td>IP address</td>
<td>Infoblox DHCP performance</td>
</tr>
<tr>
<td>Extracted Field Name</td>
<td>Description of the field</td>
<td>Values/Range</td>
<td>Source of Data</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------</td>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td>ACTION</td>
<td>Specifies the action</td>
<td>String. Example: Issued</td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>CIDR</td>
<td>Specifies the CIDR</td>
<td>Integer</td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>DEVICE_CLASS</td>
<td>Specifies the device class</td>
<td>String. Example: Linux</td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>END_EPOCH</td>
<td>Specifies the end epoch time</td>
<td>Integer</td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>FP</td>
<td>Specifies the name of the DHCP fingerprint</td>
<td>String. Example: No Match</td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>FP_CIDR</td>
<td>Specifies the fingerprint CIDR</td>
<td>Integer. Example: 8</td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>FP_NW</td>
<td>Specifies the fingerprint network</td>
<td>Network address. Example: 10.0.0.0</td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>FP_RANGE</td>
<td>Specifies the fingerprint range</td>
<td>Network range. Example: 10.0.0.0-10.0.0.200</td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>FP_VIEW</td>
<td>Specifies the fingerprint view</td>
<td>String. Example: default</td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEASE_IP</td>
<td>Specifies the lease IP address</td>
<td>IP address</td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>MAC_DUID</td>
<td>Specifies the MAC address</td>
<td>MAC address</td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>Name</td>
<td>Description of the field</td>
<td>Values/Range</td>
<td>Source of Data</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS Server</td>
<td>Specifies the MS server IP Address</td>
<td></td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>NW</td>
<td>Specifies the network Network address. Example: 10.0.0.0</td>
<td></td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>OPTION12HOST</td>
<td>Specifies the host name that is sent using DHCP Option 12 String. Example: Fedora21</td>
<td></td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>OS_NUMBER</td>
<td>Specifies the OS number Integer</td>
<td></td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>PROTO</td>
<td>Specifies the protocol String. Example: dhcpd</td>
<td></td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>SFP</td>
<td>SFP String. Example: Ubuntu/Debian 5/Knoppix 6</td>
<td></td>
<td>Infoblox DHCP fingerprint</td>
</tr>
<tr>
<td>START_EPOCH</td>
<td>Specifies the start epoch time Integer</td>
<td></td>
<td>Infoblox DHCP lease history</td>
</tr>
<tr>
<td>VIEW</td>
<td>Specifies the view</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>display_name</td>
<td>Specifies the DNS view String</td>
<td></td>
<td>DNS view lookup from dns_viewkey_displayname.csv using the View field value.</td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>punct</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>source</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sourcetype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeendpos</td>
<td>Common extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timestartpos</td>
<td>Common extracted fields</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Infoblox DDI Utilization**

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Type</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>address_alloc</td>
<td>Specifies the address allocation count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>address_assignable</td>
<td>Specifies the address assignable count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>address_assigned</td>
<td>Specifies the address assigned count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>address_conflicts</td>
<td>Specifies the address conflicts count</td>
<td></td>
<td></td>
</tr>
<tr>
<td>address_reserved</td>
<td>Specifies the address reserved count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>address_total</td>
<td>Specifies the total number of addresses</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>address_unalloc</td>
<td>Specifies the address unallocation count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>address_unmanaged</td>
<td>Specifies the address unmanaged count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>allocation</td>
<td>Allocation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cidr</td>
<td>Specifies the CIDR</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>discovered_name</td>
<td>Specifies the discovered name</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>display_name</td>
<td>Specifies the DNS view</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>first_discovered_timestamp</td>
<td>Specifies the first discovered timestamp</td>
<td>Timestamp</td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hosts</td>
<td>Specifies the address hosts count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip_address</td>
<td>Specifies the IP address</td>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>last_discovered_timestamp</td>
<td>Specifies the last discovered timestamp</td>
<td>Timestamp</td>
<td></td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>managed</td>
<td>Indicates if managed or not</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>management_platform</td>
<td>Specifies the management platform</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>members</td>
<td>Specifies the DHCP members</td>
<td>Example: infoblox.localdomain</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>ms_primary</td>
<td>Specifies the MS primary</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>port_vlan_name</td>
<td>Specifies the VLAN port name</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>port_vlan_number</td>
<td>Specifies the VLAN port number</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>network_view</td>
<td>Specifies the network view</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>primary</td>
<td>Primary</td>
<td>FQDN</td>
<td></td>
</tr>
<tr>
<td>protocol</td>
<td>Specifies the DHCP protocol</td>
<td>Example: IPV4</td>
<td></td>
</tr>
<tr>
<td>punct</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rr_a</td>
<td>Specifies the resource record A count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>rr_aaaa</td>
<td>Specifies the resource record AAAA count</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Type</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------</td>
<td>----------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>rr_cname</td>
<td>Specifies the resource record CNAME count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_dhcid</td>
<td>Specifies the resource record DHCID count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_dname</td>
<td>Specifies the resource record DNAME count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_dnskey</td>
<td>Specifies the resource record DNSKEY count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_ds</td>
<td>Specifies the resource record DS count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_lbdn</td>
<td>Specifies the resource record LBDN count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_mx</td>
<td>Specifies the resource record MX count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_naptr</td>
<td>Specifies the resource record NAPTR count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_ns</td>
<td>Specifies the resource record NS count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_nsec</td>
<td>Specifies the resource record NSEC count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_nsec3</td>
<td>Specifies the resource record NSEC3 count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_nsec3param</td>
<td>Specifies the resource record NSEC3PARAM count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_other</td>
<td>Specifies the resource record OTHER count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_ptr</td>
<td>Specifies the resource record PTR count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_rrsig</td>
<td>Specifies the resource record RRSIG count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_soa</td>
<td>Specifies the resource record SOA count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_srv</td>
<td>Specifies the resource record SRV count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_tlsa</td>
<td>Specifies the resource record TLSA count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_total</td>
<td>Specifies the resource record TOTAL count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>rr_txt</td>
<td>Specifies the resource record TXT count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>signed</td>
<td>Indicates whether signed or not</td>
<td>Boolean</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>source</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sourcetype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timestamp</td>
<td>Specifies the timestamp of the event</td>
<td>Example: 2017-02-04 03:45:53</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>utilization</td>
<td>Specifies the address utilization count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>view</td>
<td>Specifies the network view</td>
<td>Example: default</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>zone_format</td>
<td>Specifies the zone format</td>
<td>String</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>zone_name</td>
<td>Specifies the zone name</td>
<td>String</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>zones_forward</td>
<td>Specifies the zone forward count</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>zones_ipv4</td>
<td>Specifies the IPv4 count of the zone</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>zones_ipv6</td>
<td>Specifies the IPv6 count of the zone</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
<tr>
<td>zones_signed</td>
<td>Specifies the signed count of the zone</td>
<td>Integer</td>
<td>Infoblox DDI utilization</td>
</tr>
</tbody>
</table>

Infoblox Discovered Devices related dashboards/reports
<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADM_DN_OP_DN_COUNT</td>
<td>Admin-Down/Operation-DownPort Count</td>
<td>Integer</td>
</tr>
<tr>
<td>ADM_UP_OP_DN_COUNT</td>
<td>Admin-Up/Operation-UpPort Count</td>
<td>Integer</td>
</tr>
<tr>
<td>ADM_UP_OP_UP_COUNT</td>
<td>Admin-Up/Operation-DownPort Count</td>
<td>Integer</td>
</tr>
<tr>
<td>COMPONENT_NAME</td>
<td>Specifies the component name</td>
<td>String. Example: DELL-PC8024F</td>
</tr>
<tr>
<td>COMPONENT_TYPE</td>
<td>Specifies the component type</td>
<td>String. Example: Switch-Router</td>
</tr>
<tr>
<td>COMPONENT_PORT</td>
<td>Specifies the component port</td>
<td>String. Example: Gi1/0/24</td>
</tr>
<tr>
<td>DEVICE_MGMT_IP</td>
<td>Specifies the device management IP address</td>
<td>IP address</td>
</tr>
<tr>
<td>DEVICE_MODEL</td>
<td>Specifies the device model</td>
<td>String. Example: EX2200</td>
</tr>
<tr>
<td>DEVICE_NAME</td>
<td>Specifies the device name</td>
<td>String. Example: Cisco_434f44</td>
</tr>
<tr>
<td>DEVICE_TYPE</td>
<td>Specifies the device type</td>
<td>String. Example: Switch, Router</td>
</tr>
<tr>
<td>DEVICE_VENDOR</td>
<td>Specifies the device vendor</td>
<td>String. Example: Avaya</td>
</tr>
<tr>
<td>DISCOVERED_MAC_DUID</td>
<td>Specifies the discovered MAC DUID</td>
<td>MAC address</td>
</tr>
<tr>
<td>DISCOVERED_NAME</td>
<td>Specifies the discovered name</td>
<td>Example: dev_view1.yahoo.com</td>
</tr>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
</tr>
<tr>
<td>IN_USE_FLAG</td>
<td>In use flag</td>
<td>Integer. Example: 1</td>
</tr>
<tr>
<td>IPADDR</td>
<td>Specifies the IP address</td>
<td>IP Address. Example: 11.11.11.11</td>
</tr>
<tr>
<td>IPADDR_MASK</td>
<td>Specifies the IP address mask</td>
<td>Integer. Example: 128</td>
</tr>
<tr>
<td>MAC_DUID</td>
<td>Specifies the MAC address</td>
<td>MAC address</td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
</tr>
<tr>
<td>NETWORK_VIEW</td>
<td>Specifies the network view</td>
<td>String. Example: default</td>
</tr>
<tr>
<td>NON_NULL_NAME</td>
<td>Specifies the non-null name</td>
<td>String. Example: DELL-PC8024F</td>
</tr>
<tr>
<td>NON_NULL_PORT</td>
<td>Specifies the non-null port</td>
<td>String. Example: Gi1/0/24</td>
</tr>
<tr>
<td>TIMESTAMP</td>
<td>Specifies the timestamp</td>
<td>Timestamp. Example: 2017-02-15 15:56:27</td>
</tr>
<tr>
<td>TIMESTAMP_USER_HOST_</td>
<td>Specifies the timestamp userhost process pid info prefix</td>
<td></td>
</tr>
<tr>
<td>PROCESS_PID_INFO_PREFIX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL_AVAIL_COUNT</td>
<td>Specifies the total available count</td>
<td>Integer</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type</td>
<td>String</td>
</tr>
<tr>
<td>ap_bss_mac</td>
<td>Access Point BSS MAC</td>
<td>MAC address</td>
</tr>
<tr>
<td>ap_ip_dotted</td>
<td>Access Point IP dotted</td>
<td>String</td>
</tr>
<tr>
<td>ap_mac</td>
<td>Access Point MAC</td>
<td>MAC address</td>
</tr>
<tr>
<td>ap_name</td>
<td>Access Point name</td>
<td>String</td>
</tr>
<tr>
<td>ap_associated_ssid</td>
<td>Access Point associated SSID</td>
<td>String</td>
</tr>
<tr>
<td>asset_type</td>
<td>Specifies the asset type</td>
<td>String</td>
</tr>
<tr>
<td>class</td>
<td>Specifies the class name</td>
<td>String</td>
</tr>
<tr>
<td>component_name</td>
<td>Specifies the component name</td>
<td>String</td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Specifies the description</td>
<td>String</td>
</tr>
<tr>
<td>device_id</td>
<td>Specifies the device ID</td>
<td>Integer</td>
</tr>
<tr>
<td>device_ip_address</td>
<td>Specifies the device IP address</td>
<td>IP address</td>
</tr>
<tr>
<td>device_model</td>
<td>Specifies the device model</td>
<td>String</td>
</tr>
<tr>
<td>device_name</td>
<td>Specifies the device name</td>
<td>String</td>
</tr>
<tr>
<td>device_os_version</td>
<td>Specifies the device OS version</td>
<td>String</td>
</tr>
<tr>
<td>device_type</td>
<td>Specifies the device type</td>
<td>String</td>
</tr>
<tr>
<td>device_vendor</td>
<td>Specifies the device vendor</td>
<td>String</td>
</tr>
<tr>
<td>device_version</td>
<td>Specifies the device version</td>
<td>String</td>
</tr>
<tr>
<td>display_name</td>
<td>Specifies the DNS view</td>
<td>String</td>
</tr>
<tr>
<td>end_host_addl_info</td>
<td>Specifies additional information about the end host</td>
<td>String</td>
</tr>
<tr>
<td>end_host_device_model</td>
<td>Specifies the device model of the end host</td>
<td>String</td>
</tr>
<tr>
<td>end_host_device_type</td>
<td>Specifies the device type of the end host</td>
<td>String</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Data Type</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>end_host_device_vendor</td>
<td>Specifies the device vendor of the end host</td>
<td>String</td>
</tr>
<tr>
<td>end_host_first_discovered</td>
<td>Specifies the first occasion when the end host was first discovered</td>
<td>Integer</td>
</tr>
<tr>
<td>end_host_ip_address</td>
<td>Specifies the IP address of the end host</td>
<td>IP address</td>
</tr>
<tr>
<td>end_host_last_discovered</td>
<td>Indicates when was end host last discovered</td>
<td>Integer</td>
</tr>
<tr>
<td>end_host_mac_address</td>
<td>Specifies the MAC address of the end host</td>
<td>MAC address</td>
</tr>
<tr>
<td>end_host_name</td>
<td>Specifies the name of the end host</td>
<td>String</td>
</tr>
<tr>
<td>end_host_network_view</td>
<td>Specifies the network view of the end host</td>
<td>String</td>
</tr>
<tr>
<td>end_host_os_version</td>
<td>Specifies the version of the end host OS</td>
<td>String</td>
</tr>
<tr>
<td>firmware_rev</td>
<td>Indicates firmware revision</td>
<td>String</td>
</tr>
<tr>
<td>first_seen</td>
<td>First seen timestamp</td>
<td>Integer</td>
</tr>
<tr>
<td>hardware_rev</td>
<td>Specifies revision of the hardware</td>
<td>String</td>
</tr>
<tr>
<td>host</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>index</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>interface_admin_status</td>
<td>Specifies the interface admin status</td>
<td>String</td>
</tr>
<tr>
<td>interface_description</td>
<td>Specifies the interface interface description</td>
<td>String</td>
</tr>
<tr>
<td>interface_ip_address</td>
<td>Specifies the interface IP address</td>
<td>IP address</td>
</tr>
<tr>
<td>interface_name</td>
<td>Specifies the interface name</td>
<td>String</td>
</tr>
<tr>
<td>interface_port_status</td>
<td>Specifies the interface port status</td>
<td>String</td>
</tr>
<tr>
<td>interface_speed</td>
<td>Specifies the interface speed</td>
<td>Integer</td>
</tr>
<tr>
<td>interface_type</td>
<td>Specifies the interface type</td>
<td>String</td>
</tr>
<tr>
<td>interface_vlan</td>
<td>Specifies the interface VLAN ID</td>
<td>Integer</td>
</tr>
<tr>
<td>interface_vlan_name</td>
<td>Specifies the interface VLAN name</td>
<td>String</td>
</tr>
<tr>
<td>ip_address</td>
<td>Specifies the IP address</td>
<td>IP address</td>
</tr>
<tr>
<td>is_trunk_port</td>
<td>Specifies if it is a trunk port or not</td>
<td>Boolean</td>
</tr>
<tr>
<td>last_seen</td>
<td>Specifies the last seen timestamp</td>
<td>Integer</td>
</tr>
<tr>
<td>linecount</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>model</td>
<td>Specifies the model name</td>
<td>String</td>
</tr>
<tr>
<td>network_view</td>
<td>Specifies the network view</td>
<td>String</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description of the field</td>
<td>Values/Range</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>port_last_changed_at</td>
<td>The timestamp when the port was last changed</td>
<td>Timestamp</td>
</tr>
<tr>
<td>punct</td>
<td>Splunk Default field</td>
<td></td>
</tr>
<tr>
<td>serial_number</td>
<td>Specifies the serial number</td>
<td>String. Example: JPE12440180</td>
</tr>
<tr>
<td>software_rev</td>
<td>Specifies the software revision</td>
<td>String. Example: 15.2(1)E2</td>
</tr>
<tr>
<td>source</td>
<td>Splunk Default field</td>
<td></td>
</tr>
<tr>
<td>source_type</td>
<td>Splunk Default field</td>
<td></td>
</tr>
<tr>
<td>splunk_server</td>
<td>Splunk Default field</td>
<td></td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Splunk Default field</td>
<td></td>
</tr>
<tr>
<td>switch_interface</td>
<td>Specifies the switch interface</td>
<td>String. Example: Gi0/47</td>
</tr>
<tr>
<td>switch_ip_address</td>
<td>Specifies the switch IP Address</td>
<td>IP Address</td>
</tr>
<tr>
<td>switch_model</td>
<td>Indicates the switch model</td>
<td>String. Example: cat3560x48</td>
</tr>
<tr>
<td>switch_name</td>
<td>Specifies the switch name</td>
<td>String. Example: ni-mri-sw4.inca.infoblox.com</td>
</tr>
<tr>
<td>switch_os_version</td>
<td>Specifies the OS version of the switch</td>
<td>String. Example: 12.2(53)SE2</td>
</tr>
<tr>
<td>switch_type</td>
<td>Specifies the switch type</td>
<td>String. Example: Switch</td>
</tr>
<tr>
<td>switch_vendor</td>
<td>Specifies the vendor of the switch</td>
<td>String. Example: Cisco</td>
</tr>
<tr>
<td>switch_vlan</td>
<td>Specifies the switch VLAN</td>
<td>Integer. Example: 18</td>
</tr>
<tr>
<td>timeendpos</td>
<td>Common extracted fields</td>
<td></td>
</tr>
<tr>
<td>timestamp</td>
<td>Indicates the timestamp</td>
<td>Integer</td>
</tr>
<tr>
<td>timestamp_user_host_process_pid_info_prefix</td>
<td>Specifies the prefix</td>
<td>String</td>
</tr>
<tr>
<td>timetartpos</td>
<td>Common extracted fields</td>
<td></td>
</tr>
<tr>
<td>user_id</td>
<td>Specifies the User ID</td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>Specifies the DNS view</td>
<td>String</td>
</tr>
<tr>
<td>virtual_ind</td>
<td>Specifies the virtual indicator</td>
<td>Integer</td>
</tr>
</tbody>
</table>

**Infoblox Threat Protection related dashboards/reports**

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACOUNT</td>
<td>ACOUNT</td>
<td>Integer</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>ACTIVE_COUNT</td>
<td>Specifies the active count</td>
<td>Integer</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>ALERT_ID</td>
<td>Specifies the alert ID</td>
<td>Integer</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>ALERT_TYPE</td>
<td>Specifies the alert type</td>
<td>String</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>BLOCK_END</td>
<td>Specifies the block end IP address</td>
<td>Integer</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Type</td>
<td>Related Dashboards/Reports</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>BLOCK_START</td>
<td>Specifies the block start IP address</td>
<td>Integer</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>CATEGORY</td>
<td>Specifies the category</td>
<td>String. Example: OSPF</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>CLIENT</td>
<td>Specifies the client</td>
<td>String</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>COUNT</td>
<td>Specifies the count</td>
<td>Integer</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>DCOUNT</td>
<td>Specifies the DCOUNT</td>
<td>Integer</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>DNST_CATEGORY</td>
<td>Specifies the destination category</td>
<td>String</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>DOMAIN_NAME</td>
<td>Specifies the domain name</td>
<td>String</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>FIREEYE_APPLIANCE</td>
<td>Specifies the FireEye appliance</td>
<td>String</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>LOG_SEVERITY</td>
<td>Specifies log severity</td>
<td>String</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>MESSAGE</td>
<td>Specifies the message</td>
<td>String. Example: DROP OSPF unexpected</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>MITIGATION_ACTION</td>
<td>Specifies the mitigation action</td>
<td>String</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>NAT_STATUS</td>
<td>Specifies the NAT status</td>
<td>String</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>RECORD_DATA</td>
<td>Specifies the record data</td>
<td>String</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>RPZ_QNAME</td>
<td>Specifies the RPZ QNAME</td>
<td>String</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>RULE_DESCRIPTION</td>
<td>Specifies the rule description</td>
<td>String. Example: This rule drops any unexpected OSPF packets when OSPF is disabled.</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>RULE_NAME</td>
<td>Specifies the rule name</td>
<td>String. Example: DROP OSPF unexpected</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>RULE_SID</td>
<td>Specifies the rule SID</td>
<td>Integer</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>SEVERITY</td>
<td>Specifies the severity</td>
<td>String. Example: INFORMATIONAL</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>SID</td>
<td>Specifies the SID</td>
<td>Integer</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>SOURCE_IP</td>
<td>Specifies the source IP</td>
<td>IP address</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>SOURCE_PORT</td>
<td>Specifies the source port</td>
<td>Integer</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>TIMESTAMP</td>
<td>Indicates the timestamp</td>
<td>Timestamp</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>TOTAL_COUNT</td>
<td>Specifies the total count</td>
<td>Integer</td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
</tbody>
</table>

*atp_rule_sid_lookup* lookup from `/tmp/reporting_atp_conf/atp_rule_sid_lookup.csv` with RULE_SID value as input.
<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox DNS traffic control</td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox DNS traffic control</td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox DNS traffic control</td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox DNS traffic control</td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox DNS traffic control</td>
</tr>
<tr>
<td>available</td>
<td>Specifies the available count</td>
<td>Integer</td>
<td>Infoblox DNS traffic control</td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>punct</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>source</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>splunk_server</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
<tr>
<td>timestartpos</td>
<td>Common extracted fields</td>
<td></td>
<td>Infoblox threat protection related dashboards/reports</td>
</tr>
</tbody>
</table>

**Infoblox DNS Traffic Control**

Most of the fields in this index are extracted directly from the `syslog_filtered.log` file. Some of them are mentioned in the table below:
<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTION</td>
<td>Specifies the action</td>
<td>String, Example: Allocated</td>
<td>Evaluated based on the action field value</td>
</tr>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TENANT_NAME</td>
<td>Specifies the name of the tenant associated with the VM</td>
<td>String</td>
<td>tenant_name_lookup lookup from /storage/splunk/etc/apps/infoblox/lookups/tenant_name_lookup.csv with tenant_id value as input</td>
</tr>
<tr>
<td>action</td>
<td>Specifies the action count</td>
<td>Integer</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>address</td>
<td>Specifies the IP address</td>
<td>IP address</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>address_type</td>
<td>Specifies the type of address</td>
<td>Integer</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>application_type</td>
<td>Specifies the application type</td>
<td></td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>cidr</td>
<td>Specifies the CIDR</td>
<td>Example: 24</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>cnames</td>
<td>Specifies the common name</td>
<td>String</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>display_name</td>
<td>Specifies the DNS view</td>
<td>String</td>
<td>DNS view lookup from dns_viewkey_displayname.csv using the VIEW field value</td>
</tr>
<tr>
<td>Extracted Field Name</td>
<td>Description of the field</td>
<td>Values/Range</td>
<td>Source of Data</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------</td>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td>elastic_address</td>
<td>Specifies the elastic IP address</td>
<td>IP address</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>Fqdn</td>
<td>Specifies the FQDN</td>
<td>String</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>interface_name</td>
<td>Specifies the interface name</td>
<td>String</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>is_primary_ifc</td>
<td>Indicates if primary IFC or not</td>
<td>Example: 0 (not primary)</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>location</td>
<td>Specifies the location</td>
<td></td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>mac_address</td>
<td>Specifies the MAC address</td>
<td>Example: 00:11:22:33:44:55</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>mgmt_platform</td>
<td>Specifies management platform</td>
<td>Example: vm132ctest</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>network</td>
<td>Specifies the network address</td>
<td>Example: 10.0.0.0/8</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>network_view</td>
<td>Specifies the network view</td>
<td>Example: default</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>port_id</td>
<td>Specifies the port ID</td>
<td>Integer</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>private_address</td>
<td>Specifies the private address</td>
<td>IP address</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>private_hostname</td>
<td>Specifies the private hostname</td>
<td>String</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>public_address</td>
<td>Specifies the public address</td>
<td>IP address</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>public_hostname</td>
<td>Specifies the public hostname</td>
<td>String</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>punct</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>source</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>splunk_server</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Splunk Default field</td>
<td></td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>tenant_id</td>
<td>Specifies the tenant ID</td>
<td>Integer</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>timeendpos</td>
<td>Common extracted fields</td>
<td></td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>timestamp</td>
<td>Indicates the timestamp of the event</td>
<td>Example: 2017-02-04 03:45:53</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>timestamppos</td>
<td>Common extracted fields</td>
<td></td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>view</td>
<td>Specifies the DNS view</td>
<td>String</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>vlan_id</td>
<td>Specifies the VLAN ID</td>
<td>Integer</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>vm_hostname</td>
<td>Specifies the hostname of the VM</td>
<td>String</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>vm_name</td>
<td>Specifies the name of the VM</td>
<td>Example: 99</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>vm_vpc_address</td>
<td>Specifies the VPC address of the VM</td>
<td>IP address</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>vm_vpc_cidr</td>
<td>Specifies the VPC CIDR of the VM</td>
<td>Example: 24</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>vm_vpc_id</td>
<td>Specifies the VPC ID of the VM</td>
<td>Integer</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>vm_vpc_name</td>
<td>Specifies the VPC name of the VM</td>
<td>Integer</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
<tr>
<td>vpc_addr</td>
<td>Specifies the VPC address of the VM</td>
<td>IP address</td>
<td>Infoblox cloud related dashboards/reports</td>
</tr>
</tbody>
</table>

**Infoblox Syslog**

Most of the fields in this index are extracted directly from the `syslog_filtered.log` file. Some of them are mentioned in the table below:

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
</table>

Copyright ©2019, Infoblox, Inc. All right reserved.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>COUNT</td>
<td>Specifies the count</td>
<td>Integer</td>
<td>System capacity</td>
</tr>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>group</td>
<td>Example: admin-group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hits</td>
<td>Integer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>misses</td>
<td>Integer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>punct</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>size</td>
<td>Integer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>source</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sourcetype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeendpos</td>
<td>Common extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timestartpos</td>
<td>Common extracted fields</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

System Capacity

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>COUNT</td>
<td>Specifies the count</td>
<td>Integer</td>
<td>System capacity</td>
</tr>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PERCENT</td>
<td>Specifies the percentage</td>
<td>Integer</td>
<td>System capacity</td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Infoblox System Utilization (CPU, Memory, Network Traffic) related dashboards/reports

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU_PERCENT</td>
<td>Specifies the CPU percentage</td>
<td>Integer value within 0-100</td>
<td>Infoblox system utilization related dashboards/reports</td>
</tr>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMORY_PERCENT</td>
<td>Specifies the memory percentage</td>
<td>Integer. Value within 0-100</td>
<td>Infoblox system utilization related dashboards/reports</td>
</tr>
<tr>
<td>TRAF_VALUE</td>
<td>Specifies the traffic value</td>
<td>Integer</td>
<td>Infoblox system utilization related dashboards/reports</td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extracted Field Name</td>
<td>Description of the field</td>
<td>Values/Range</td>
<td>Source of Data</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------</td>
<td>-------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>punct</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>source</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sourcetype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sys_report_id</td>
<td>Specifies the report ID based on whether inbound or outbound</td>
<td>Integer</td>
<td>Infoblox system utilization related dashboards/reports</td>
</tr>
<tr>
<td>timeendpos</td>
<td>Common extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timestartpos</td>
<td>Common extracted fields</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Infoblox Ecosystem Subscription**

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cisco_ise_endpoint_profile</td>
<td>Specifies the Cisco ISE endpoint profile</td>
<td>String</td>
<td>Infoblox ecosystem subscription</td>
</tr>
<tr>
<td>cisco_ise_security_group</td>
<td>Specifies the Cisco ISE security group</td>
<td></td>
<td>Infoblox ecosystem subscription</td>
</tr>
<tr>
<td>cisco_ise_session_state</td>
<td>Specifies the Cisco ISE session state</td>
<td>String, Example: STARTED</td>
<td>Infoblox ecosystem subscription</td>
</tr>
<tr>
<td>cisco_ise_ssid</td>
<td>Specifies the Cisco ISE SSID</td>
<td>String</td>
<td>Infoblox ecosystem subscription</td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>domainname</td>
<td>Specifies the domain name</td>
<td>String</td>
<td>Infoblox ecosystem subscription</td>
</tr>
<tr>
<td>ea_eps_status</td>
<td>Specifies the EPS status of the extensible attribute</td>
<td>String</td>
<td>Infoblox ecosystem subscription</td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>guid</td>
<td>Specifies the GUID</td>
<td>String</td>
<td>Infoblox ecosystem subscription</td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip_address</td>
<td>Specifies the IP address</td>
<td>IP address</td>
<td>Infoblox ecosystem subscription</td>
</tr>
<tr>
<td>last_discovered_timestamp</td>
<td>Specifies the last discovered timestamp</td>
<td>Integer</td>
<td>Infoblox ecosystem subscription</td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field Name</td>
<td>Description of the field</td>
<td>Values/Range</td>
<td>Source of Data</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>--------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>port_vlan_name</td>
<td>Specifies the VLAN name of the port</td>
<td>String</td>
<td>Infoblox ecosystem subscription</td>
</tr>
<tr>
<td>port_vlan_number</td>
<td>Specifies the VLAN number of the port</td>
<td>Integer</td>
<td>Infoblox ecosystem subscription</td>
</tr>
<tr>
<td>punct</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>source</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>splunk_server</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>timeendpos</td>
<td>Common extracted fields</td>
<td></td>
<td>Common extracted fields</td>
</tr>
<tr>
<td>timestamp</td>
<td>Specifies the timestamp of the event</td>
<td>Example: 2017-02-04 03:45:53</td>
<td>Infoblox ecosystem subscription</td>
</tr>
<tr>
<td>user</td>
<td>Specifies the username</td>
<td>String</td>
<td>Infoblox ecosystem subscription</td>
</tr>
<tr>
<td>username</td>
<td>Specifies the username</td>
<td>String</td>
<td>Infoblox ecosystem subscription</td>
</tr>
</tbody>
</table>

**Infoblox Ecosystem Publication**

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox ecosystem publication</td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox ecosystem publication</td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox ecosystem publication</td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox ecosystem publication</td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox ecosystem publication</td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td>Infoblox ecosystem publication</td>
</tr>
<tr>
<td>contents</td>
<td>Specifies the content</td>
<td>String, Example: {'LEASE_STATE': 'STARTED', 'Lease_Start_Time': '2017-03-01T07:00:00Z', 'MAC_OR_DUID': '80:3c:3e:29:84:cc', 'Fingerprint': 'No Match', 'Lease_End_Time': '2017-03-01T07:02:00Z', 'IPAddress': '10.0.0.20', 'Infoblox_Member': '10.35.205.6'}</td>
<td>Infoblox ecosystem publication</td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>ip_address</td>
<td>Specifies the IP address</td>
<td>IP address</td>
<td>Infoblox ecosystem publication</td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>notification_action</td>
<td>Specifies the notification action</td>
<td>Example: CISCOISE_PUBLISH_IPAM</td>
<td>Infoblox ecosystem publication</td>
</tr>
</tbody>
</table>
### Reporting License Usage

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Source of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA</td>
<td></td>
<td></td>
<td>Common Extracted fields</td>
</tr>
<tr>
<td>HWTYPE</td>
<td></td>
<td></td>
<td>Common Extracted fields</td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td></td>
<td></td>
<td>Common Extracted fields</td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td></td>
<td></td>
<td>Common Extracted fields</td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td></td>
<td></td>
<td>Common Extracted fields</td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td></td>
<td></td>
<td>Common Extracted fields</td>
</tr>
<tr>
<td>date_hour</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_mday</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_minute</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_month</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_second</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_wday</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_year</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>date_zone</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>display_name</td>
<td>Specifies the DNS view</td>
<td>String</td>
<td>DNS view lookup from dns_viewkey_displayname.csv using the View field value</td>
</tr>
<tr>
<td>eventtype</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>host</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>index</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>license_count</td>
<td>Specifies the license count</td>
<td>Integer</td>
<td>Reporting license usage</td>
</tr>
<tr>
<td>license_pool</td>
<td>Specifies the license pool</td>
<td>String, Example: cloud_api.0</td>
<td>Reporting license usage</td>
</tr>
<tr>
<td>linecount</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>punct</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>source</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>sourcetype</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>splunk_server</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>splunk_server_group</td>
<td></td>
<td></td>
<td>Splunk Default field</td>
</tr>
<tr>
<td>timeendpos</td>
<td></td>
<td></td>
<td>Common extracted fields</td>
</tr>
<tr>
<td>timestamp</td>
<td>Indicates the timestamp</td>
<td>Timestamp</td>
<td>Reporting license usage</td>
</tr>
<tr>
<td>timestartpos</td>
<td></td>
<td></td>
<td>Common extracted fields</td>
</tr>
<tr>
<td>Summary Index</td>
<td>Report</td>
<td>Frequency</td>
<td>Cron Schedule</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>ib_dns_summary</td>
<td>si_dns_reclaimed_object_count_trend</td>
<td>At every 30th minute from 21 through 59</td>
<td>21-59/30 * * *</td>
</tr>
<tr>
<td>si_dns_top_clients</td>
<td></td>
<td>At every 30th minute from 2 through 59</td>
<td>2-59/30 * * *</td>
</tr>
<tr>
<td>si_dns_query_reply</td>
<td></td>
<td>At every 30th minute from 18 through 59</td>
<td>18-59/30 * * *</td>
</tr>
<tr>
<td>si_top_servfail_received_queries</td>
<td></td>
<td>At every 30th minute from 7 through 59</td>
<td>7-59/30 * * *</td>
</tr>
<tr>
<td>si_dns_response_latency_trend</td>
<td></td>
<td>At every 30th minute from 20 through 59</td>
<td>20-59/30 * * *</td>
</tr>
<tr>
<td>si_dns_member_qps_trend_per_hour</td>
<td></td>
<td>At minute 34</td>
<td>34 * * *</td>
</tr>
<tr>
<td>si_top_nxdomain_query</td>
<td></td>
<td>At every 30th minute from 5 through 59</td>
<td>5-59/30 * * *</td>
</tr>
<tr>
<td>si_dns_member_qps_trend_per_day</td>
<td></td>
<td>Every day 32 minutes past midnight</td>
<td>32 0 * * *</td>
</tr>
<tr>
<td>si_dns_member_qps_trend</td>
<td></td>
<td>At every 30th minute from 12 through 59</td>
<td>12-59/30 * * *</td>
</tr>
<tr>
<td>si_dns_requested_domain</td>
<td></td>
<td>At every 30th minute from 4 through 59</td>
<td>4-59/30 * * *</td>
</tr>
<tr>
<td>si_dns_qps_trend</td>
<td></td>
<td>At every 30th minute from 10 through 59</td>
<td>10-59/30 * * *</td>
</tr>
<tr>
<td>si_top_servfail_sent_queries</td>
<td></td>
<td>At every 30th minute from 6 through 59</td>
<td>6-59/30 * * *</td>
</tr>
<tr>
<td>si_ddns_update</td>
<td></td>
<td>At every 30th minute from 6 through 59</td>
<td>6-59/30 * * *</td>
</tr>
<tr>
<td>si_dns_cache_hit_ratio</td>
<td></td>
<td>At every 30th minute from 8 through 59</td>
<td>8-59/30 * * *</td>
</tr>
<tr>
<td>si_top_timeout_queries</td>
<td></td>
<td>At every 30th minute from 8 through 59</td>
<td>8-59/30 * * *</td>
</tr>
<tr>
<td>si_dns_rpz_hits</td>
<td></td>
<td>At every 10th minute from 2 through 59</td>
<td>2-59/10 * * *</td>
</tr>
<tr>
<td>si_top_clients_per_domain</td>
<td></td>
<td>At every 30th minute from 3 through 59</td>
<td>3-59/30 * * *</td>
</tr>
<tr>
<td>ib_dhcp_summary</td>
<td>si_dhcp_message</td>
<td>At every 30th minute from 14 through 59</td>
<td>14-59/30 * * *</td>
</tr>
<tr>
<td>si_dhcp_usage_trend</td>
<td></td>
<td>At 22 minutes past every 8th hour</td>
<td>22 */8 * * *</td>
</tr>
<tr>
<td>si_dhcp_top_lease_client</td>
<td></td>
<td>At every 30th minute from 16 through 59</td>
<td>16-59/30 * * *</td>
</tr>
<tr>
<td>si_devices_denied_an_ip_address</td>
<td></td>
<td>At every 30th minute from 19 through 59</td>
<td>19-59/30 * * *</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description of the field</td>
<td>Values/Range</td>
<td>Remarks</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>si_dhcp_range_utilization_trend</td>
<td>At 24 minutes past every 8th hour</td>
<td>24 */8 * * *</td>
<td>15m@m 495m@m</td>
</tr>
<tr>
<td>si_dhcp_top_os_by_network</td>
<td>At every 30th minute from 16 through 59</td>
<td>16-59/30 * * *</td>
<td>30m@m 60m@m</td>
</tr>
<tr>
<td>si_dhcp_top_os_by_network</td>
<td>At every 30th minute from 16 through 59</td>
<td>16-59/30 * * *</td>
<td>30m@m 60m@m</td>
</tr>
<tr>
<td>ib_dtc_summary</td>
<td>si_dtc_response_distribution</td>
<td>At 37 minutes past every 6th hour</td>
<td>37 */6 * * *</td>
</tr>
<tr>
<td>si_adns_resource_pool_availability</td>
<td>At 23 minutes past every 6th hour</td>
<td>23 */6 * * *</td>
<td>10m@m 370m@m</td>
</tr>
<tr>
<td>si_smart_dns_resource_snmp</td>
<td>At 47 minutes past every 6th hour</td>
<td>47 */6 * * *</td>
<td>10m@m 370m@m</td>
</tr>
<tr>
<td>si_smart_dns_resource_availability</td>
<td>At 47 minutes past every 6th hour</td>
<td>47 */6 * * *</td>
<td>10m@m 370m@m</td>
</tr>
<tr>
<td>ib_system_summary</td>
<td>si_index_disk_usage</td>
<td>At 37 minutes past every 6th hour</td>
<td>37 */6 * * *</td>
</tr>
<tr>
<td>si_memory_utilization</td>
<td>At every 30th minute from 26 through 59</td>
<td>26-59/30 * * *</td>
<td>30m@m 60m@m</td>
</tr>
<tr>
<td>si_traffic_rate</td>
<td>At every 30th minute from 28 through 59</td>
<td>28-59/30 * * *</td>
<td>30m@m 60m@m</td>
</tr>
<tr>
<td>si_cpu_usage</td>
<td>At every 30th minute</td>
<td>*/30 * * *</td>
<td>30m@m 60m@m</td>
</tr>
<tr>
<td>ib_security_summary</td>
<td>si_dns_tunneling_activity</td>
<td>At every 3030th minute from 11 through 59</td>
<td>11-59/30 * * *</td>
</tr>
</tbody>
</table>

**Note:**
- **cron schedule** - cron time scheduled to execute a search
- **earliest time** - specifies the earliest time for a search
- **latest time** - specifies the latest time for a saved search

### Common fields in summary indexes

Splunk server adds the following fields to every event in each summary index.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description of the field</th>
<th>Values/Range</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>info_max_time</td>
<td>The info_* fields are added to each event when you use the addinfo command. This command is primarily an internally-used component of Summary Indexing. Click here for more information. The latest time boundary for the search.</td>
<td>Integer</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>info_min_time</td>
<td>Specifies the earliest time boundary for search</td>
<td>Integer</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>info_search_time</td>
<td>Specifies the time when search was initiated</td>
<td>Integer</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>search_name</td>
<td>Specifies the name of the saved search</td>
<td>Example: si-search-dns-query-reply</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>search_now</td>
<td>Specifies the time when search was scheduled to run</td>
<td>Integer</td>
<td>Splunk added special field</td>
</tr>
</tbody>
</table>

### Infoblox DNS Summary

Note: "psrsvd" stands for "prestats reserved". Syntax is psrsvd_[\(type\)][\(fieldname\)]. These special fields are added by Splunk to summary index data that begins with "psrsvd" when you initiate search using the "si**" command to populate a summary index. See List of available psrsvd types from Splunk docs.

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Reports</th>
<th>Values/Range</th>
<th>Source of Data</th>
<th>Remarks</th>
</tr>
</thead>
</table>

Copyright ©2019, Infoblox, Inc. All right reserved.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CLIENT</strong></td>
<td>Specifies the IP address of the DNS client</td>
<td>si_dns_top_clients</td>
<td>Integer</td>
</tr>
<tr>
<td><strong>COUNT</strong></td>
<td>Specifies the count of DNS queries</td>
<td>si_top_servfail_received_queries</td>
<td>Integer</td>
</tr>
<tr>
<td><strong>EA</strong></td>
<td>Specifies the average count of DNS RPX hits</td>
<td>si_top_timeout_queries</td>
<td>Integer</td>
</tr>
<tr>
<td><strong>FQDN</strong></td>
<td>Specifies the fully qualified domain name</td>
<td>si_dns_requested_domain and si_top_clients_per_domain</td>
<td>Example: 213.31.102.10.in-a.ddr.arpa</td>
</tr>
<tr>
<td><strong>HWTYPE</strong></td>
<td>Specifies the DNS response type</td>
<td>si_dns_query_reply, si_dns_qps_trend, and si_ddns_update</td>
<td>SUCCESS/NOERROR OR REFERRAL OR NXRRSET OR NXDOMAIN OR REFUSED OR OTHER</td>
</tr>
<tr>
<td><strong>MEMBER</strong></td>
<td>Specifies the member</td>
<td>String</td>
<td>Infoblox DNS Summary</td>
</tr>
<tr>
<td><strong>MEMBER_IP</strong></td>
<td>Specifies the DNS clients per domain</td>
<td>si_top_clients_per_domain</td>
<td>Integer</td>
</tr>
<tr>
<td><strong>TLD</strong></td>
<td>Specifies top level domain names</td>
<td>si_dns_requested_domain</td>
<td>Example: .arpa</td>
</tr>
<tr>
<td><strong>TYPE</strong></td>
<td>Specifies the DNS response type</td>
<td>si_dns_query_reply, si_dns_qps_trend, and si_ddns_update</td>
<td>SUCCESS/NOERROR OR REFERRAL OR NXRRSET OR NXDOMAIN OR REFUSED OR OTHER</td>
</tr>
<tr>
<td><strong>VIEW</strong></td>
<td>It refers to the DNS view key to map DNS view through lookup. See display_name field</td>
<td>si_dns_requested_domain, si_dns_top_clients, si_dns_member_qps_trend_per_hour, si_dns_member_qps_trend_per_day, si_dns_member_qps_trend, si_dns_qps_trend, si_ddns_update, si_dns_cache_hit_ratio, si_dns_rpz_hits, si_top_clients_per_domain, si_top_timeout_queries, si_top_servfail_sent_queries, si_top_nxdomain_query, and si_top_servfail_received_queries</td>
<td>Example: _default</td>
</tr>
<tr>
<td><strong>date_hour</strong></td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Example</td>
<td>Look up from</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------</td>
<td>---------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>display_name</td>
<td>Specifies the DNS view</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_dns_requested_domain,</td>
<td></td>
<td>dns_viewkey</td>
</tr>
<tr>
<td></td>
<td>si_dns_top_clients,</td>
<td></td>
<td>_displayname</td>
</tr>
<tr>
<td></td>
<td>si_dns_member_qps_trend_per_hour,</td>
<td></td>
<td>.csv</td>
</tr>
<tr>
<td></td>
<td>si_dns_member_qps_trend_per_day,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_dns_member_qps_trend,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_dns_qps_trend,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_ddns_update,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_dns_cache_hit_ratio,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_dns_rpz_hits,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_top_clients_per_domain,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_top_timeout_queries,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_top_servfail_sent_queries,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_top_nxdomain_query,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_top_servfail_received_queries,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>default.MS-2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lookup from dns_viewkey_displayname.csv</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>using the VIEW field value.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_max_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_min_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_search_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>orig_host</td>
<td>Specifies the host name of the data source</td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>infoblox.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Splunk added default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_COUNT</td>
<td>Here, ct = count. It contains</td>
<td>si_dns_query_reply and</td>
<td>Splunk added</td>
</tr>
<tr>
<td></td>
<td>the count information for the COUNT field.</td>
<td>si_dns_qps_trend</td>
<td>special field</td>
</tr>
<tr>
<td>psrsvd_ct_LATENCY</td>
<td>Contains the count information</td>
<td>si_dns_response_latency_trend</td>
<td>Splunk added</td>
</tr>
<tr>
<td></td>
<td>for the LATENCY field</td>
<td></td>
<td>special field</td>
</tr>
<tr>
<td>psrsvd_ct_QCOUNT</td>
<td>Contains the count information</td>
<td>si_dns_member_qps_trend_per</td>
<td>Splunk added</td>
</tr>
<tr>
<td></td>
<td>for the QCOUNT field</td>
<td>_hour,</td>
<td>special field</td>
</tr>
<tr>
<td></td>
<td>and si_dns_member_qps_trend</td>
<td>si_dns_member_qps_trend_per</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>_day,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>si_dns_qps_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_gc</td>
<td>Here, gc = group count. It indicates the count</td>
<td>si_dns_query_reply,</td>
<td>Splunk added</td>
</tr>
<tr>
<td></td>
<td>for stats grouping and it is not scoped to a</td>
<td>si_dns_response_latency_trend,</td>
<td>special field</td>
</tr>
<tr>
<td></td>
<td>single field.</td>
<td>si_dns_member_qps_trend_per</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>_hour,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>si_dns_member_qps_trend_per</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>_day,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>si_dns_member_qps_trend,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>si_dns_qps_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_COUNT</td>
<td>Here, nc = numerical count. It indicates the</td>
<td>si_dns_query_reply and</td>
<td>Splunk added</td>
</tr>
<tr>
<td></td>
<td>number of numerical values and contains the</td>
<td>si_dns_qps_trend</td>
<td>special field</td>
</tr>
<tr>
<td></td>
<td>numerical count information for the COUNT</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>field.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright ©2019, Infoblox, Inc. All right reserved.
<table>
<thead>
<tr>
<th>psrsvd_nc_LATENCY</th>
<th>Contains the numerical count information for the LATENCY field</th>
<th>si_dns_response_latency_trend</th>
<th>Splunk added special field</th>
</tr>
</thead>
<tbody>
<tr>
<td>psrsvd_nc_QCOUN T</td>
<td>Contains the numerical count information for the QCOUNT field</td>
<td>si_dns_member_qps_trend_per_hour, si_dns_member_qps_trend_per_day, and si_dns_member_qps_trend</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_nx_QCOUN T</td>
<td>Here, nx = maximum numerical value. It contains the maximum numerical value information for the QCOUNT field.</td>
<td>si_dns_member_qps_trend_per_hour and si_dns_member_qps_trend_per_day</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_sm_COUNT</td>
<td>Here, sm = sum. It contains the sum information for the COUNT field.</td>
<td>si_dns_query_reply and si_dns_qps_trend</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_sm_LATENCY</td>
<td>Contains the sum information for the LATENCY field.</td>
<td>si_dns_response_latency_trend</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_sm_QCOUN T</td>
<td>Contains the sum information for the QCOUNT field</td>
<td>si_dns_member_qps_trend_per_hour, si_dns_member_qps_trend_per_day, and si_dns_member_qps_trend</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_sx_QCOUN T</td>
<td>Here, sx = maximum lexicographical value. It contains the maximum lexicographical value information for the QCOUNT field.</td>
<td>si_dns_member_qps_trend_per_hour and si_dns_member_qps_trend_per_day</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_v</td>
<td>Here, v = version. This is not scoped to a single field.</td>
<td>si_dns_query_reply, si_dns_response_latency_trend, si_dns_member_qps_trend_per_hour, si_dns_member_qps_trend_per_day, si_dns_member_qps_trend and si_dns_qps_trend</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_vt_COUNT</td>
<td>Here, vt = value type. It contains precision of the associated field. This field contains precision of the COUNT field.</td>
<td>si_dns_query_reply and si_dns_qps_trend</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_vt_LATENCY</td>
<td>Contains precision of the LATENCY field</td>
<td>si_dns_response_latency_trend</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_vt_QCOUN T</td>
<td>Contains precision of the QCOUNT field</td>
<td>si_dns_member_qps_trend_per_hour, si_dns_member_qps_trend_per_day, and si_dns_member_qps_trend</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>report</td>
<td>Contains the name of the report that populates the summary index</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Scavenge Object Count Trend data</td>
<td>si_dns_reclaimed_object_count_trend</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top Clients report data</td>
<td>si_dns_top_clients</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Replies Trend data</td>
<td>si_dns_query_reply</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top SERVFAIL Errors Received Report data</td>
<td>si_top_servfail_received_querries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Response Latency Trend data</td>
<td>si_dns_response_latency_trend</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Daily Peak Hour Query Rate by Member Report data</td>
<td>si_dns_member_qps_trend_per_hour</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Description</td>
<td>Report Name</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>DNS Top NXDOMAIN / NOERROR (no data) Report data</td>
<td>si_top_nxdomain_query</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Daily Query Rate by Member Report data</td>
<td>si_dns_member_qps_trend_per_day</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Query Rate by Member Report data</td>
<td>si_dns_member_qps_trend</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top Requested Domain Names Report data</td>
<td>si_dns_requested_domain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Queries Per Second Trend data</td>
<td>si_dns_qps_trend</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top SERVFAIL Errors Sent Report data</td>
<td>si_top_servfail_sent_queries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DDNS Update Rate Trend data</td>
<td>si_ddns_update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Cache Hit Rate Trend data</td>
<td>si_dns_cache_hit_ratio</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top Timed-Out Recursive Queries Report data</td>
<td>si_top_timeout_queries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS RPZ Hits Reports data</td>
<td>si_dns_rpz_hits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Top Clients per Domain Report data</td>
<td>si_top_clients_per_domain</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Infoblox DHCP Summary**

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Reports</th>
<th>Values/Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTION</td>
<td>Specifies the action</td>
<td></td>
<td>String. Exam</td>
</tr>
<tr>
<td>DEVICE_CLASS</td>
<td>Specifies the device class</td>
<td></td>
<td>String. Exam</td>
</tr>
<tr>
<td>DHCP_RANGE</td>
<td>Specifies the DHCP range</td>
<td></td>
<td>Network range 10.0.0.1-10.0.0.255</td>
</tr>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FP</td>
<td>Specifies the fingerprint data</td>
<td></td>
<td>String. Exam</td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEASED_IP</td>
<td>Specifies the lease IP address</td>
<td></td>
<td>IP address</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Example</td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------</td>
<td>----------------------------------</td>
<td></td>
</tr>
<tr>
<td>MAC_DUID</td>
<td>Specifies the MAC address</td>
<td>MAC address</td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Specifies the DHCP protocol</td>
<td>String. Example: IPV4</td>
<td></td>
</tr>
<tr>
<td>SFP</td>
<td>Specifies the SFP</td>
<td>String. Example: Ubuntu/Debian</td>
<td></td>
</tr>
<tr>
<td>VIEW</td>
<td>It refers to the DNS view key to map the DNS view through lookup. See display_name field</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dhcp_utilization_status</td>
<td>Specifies the DHCP utilization status</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>display_name</td>
<td>Specifies the DNS view</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>end_address</td>
<td>Specifies the end IP address</td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_max_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_min_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_search_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>members</td>
<td>Specifies the DHCP member</td>
<td>String. Example: infoblox.localdomain</td>
<td></td>
</tr>
<tr>
<td>ms_servers</td>
<td>Specifies the MS servers</td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>orig_host</td>
<td>Specifies the host name of the data source</td>
<td>Example: infoblox.com</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_FREE_ADDRESSES</td>
<td>Specifies the count information for FREE_ADDRESSES field</td>
<td>si_dhcp_usage_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_dhcp_utilization</td>
<td>Specifies the count for dhcp_utilization field</td>
<td>si_dhcp_range_utilization_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_dynamic_hosts</td>
<td>Specifies the count for dynamic_hosts field</td>
<td>si_dhcp_usage_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_static_hosts</td>
<td>Specifies the count for static_hosts field</td>
<td>si_dhcp_usage_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v4ack</td>
<td>Specifies the count for v4ack field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v4decline</td>
<td>Specifies the count for v4decline field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v4discover</td>
<td>Specifies the count for v4discover field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v4inform</td>
<td>Specifies the count for v4inform field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v4leaseactive</td>
<td>Specifies the count for v4leaseactive field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v4leasequery</td>
<td>Specifies the count for v4leasequery field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v4leaseunassigned</td>
<td>Specifies the count for v4leaseunassigned field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v4leaseunknown</td>
<td>Specifies the count for v4leaseunknown field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v4nak</td>
<td>Specifies the count for v4nak field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v4offer</td>
<td>Specifies the count for v4offer field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v4release</td>
<td>Specifies the count for v4release field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v4request</td>
<td>Specifies the count for v4request field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6advertise</td>
<td>Specifies the count for v6advertise field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6confirm</td>
<td>Specifies the count for v6confirm field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6decline</td>
<td>Specifies the count for v6decline field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6information_request</td>
<td>Specifies the count for v6information_request field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6leasequery</td>
<td>Specifies the count for v6leasequery field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6leasequery_reply</td>
<td>Specifies the count for v6leasequery_reply field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6rebind</td>
<td>Specifies the count for v6rebind field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6reconfigure</td>
<td>Specifies the count for v6reconfigure field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6relay_forward</td>
<td>Specifies the count for v6relay_forward field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6relay_reply</td>
<td>Specifies the count for v6relay_reply field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6release</td>
<td>Specifies the count for v6release field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6renew</td>
<td>Specifies the count for v6renew field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6reply</td>
<td>Specifies the count for v6reply field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6request</td>
<td>Specifies the count for v6request field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_v6solicit</td>
<td>Specifies the count for v6solicit field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_gc</td>
<td>Here, gc = group count. The count for stats grouping and not scoped to a single field.</td>
<td>si_dhcp_usage_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_FREE_ADDRESSES</td>
<td>Specifies the numerical count for FREE_ADDRESSES field</td>
<td>si_dhcp_usage_trend</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Usage</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_dhcp_utilization</td>
<td>Specifies the numerical count for dhcp_utilization field</td>
<td>si_dhcp_range_utilization_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_dynamic_hosts</td>
<td>Specifies the numerical count for dynamic_hosts field</td>
<td>si_dhcp_usage_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_static_hosts</td>
<td>Specifies the numerical count for static_hosts field</td>
<td>si_dhcp_usage_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v4ack</td>
<td>Specifies the numerical count for v4ack field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v4decline</td>
<td>Specifies the numerical count for v4decline field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v4discover</td>
<td>Specifies the numerical count for v4discover field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v4inform</td>
<td>Specifies the numerical count for v4inform field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v4leaseactive</td>
<td>Specifies the numerical count for v4leaseactive field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v4leasequery</td>
<td>Specifies the numerical count for v4leasequery field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v4leaseunassigned</td>
<td>Specifies the numerical count for v4leaseunassigned field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v4leaseunknown</td>
<td>Specifies the numerical count for v4leaseunknown field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v4nak</td>
<td>Specifies the numerical count for v4nak field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v4offer</td>
<td>Specifies the numerical count for v4offer field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v4release</td>
<td>Specifies the numerical count for v4release field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v4request</td>
<td>Specifies the numerical count for v4request field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6advertise</td>
<td>Specifies the numerical count for v6advertise field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6confirm</td>
<td>Specifies the numerical count for v6confirm field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6decline</td>
<td>Specifies the numerical count for v6decline field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6information_request</td>
<td>Specifies the numerical count for v6information_request field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6leasequery</td>
<td>Specifies the numerical count for v6leasequery field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6leasequery_reply</td>
<td>Specifies the numerical count for v6leasequery_reply field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6rebind</td>
<td>Specifies the numerical count for v6rebind field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6reconfigure</td>
<td>Specifies the numerical count for v6reconfigure field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6relay_forward</td>
<td>Specifies the numerical count for v6relay_forward field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6relay_reply</td>
<td>Specifies the numerical count for v6relay_reply field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6release</td>
<td>Specifies the numerical count for v6release field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6renew</td>
<td>Specifies the numerical count for v6renew field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6reply</td>
<td>Specifies the numerical count for v6reply field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6request</td>
<td>Specifies the numerical count for v6request field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------</td>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_v6solicit</td>
<td>Specifies the numerical count for v6solicit field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_FREE_ADDRESSES</td>
<td>Specifies the sum for FREE_ADDRESSES field</td>
<td>si_dhcp_usage_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_dhcp_utilization</td>
<td>Specifies the sum for dhcp_utilization field</td>
<td>si_dhcp_range_utilization_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_dynamic_hosts</td>
<td>Specifies the sum for dynamic_hosts field</td>
<td>si_dhcp_usage_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_static_hosts</td>
<td>Specifies the sum for static_hosts field</td>
<td>si_dhcp_usage_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v4ack</td>
<td>Specifies the sum for v4ack field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v4decline</td>
<td>Specifies the sum for v4decline field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v4discover</td>
<td>Specifies the sum for v4discover field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v4inform</td>
<td>Specifies the sum for v4inform field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v4leaseactive</td>
<td>Specifies the sum for v4leaseactive field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v4leasequery</td>
<td>Specifies the sum for v4leasequery field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v4leaseunassigned</td>
<td>Specifies the sum for v4leaseunassigned field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v4leaseunknown</td>
<td>Specifies the sum for v4leaseunknown field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v4nak</td>
<td>Specifies the sum for v4nak field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v4offer</td>
<td>Specifies the sum for v4offer field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v4release</td>
<td>Specifies the sum for v4release field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v4request</td>
<td>Specifies the sum for v4request field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v6advertise</td>
<td>Specifies the sum for v6advertise field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v6confirm</td>
<td>Specifies the sum for v6confirm field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v6leasequery</td>
<td>Specifies the sum for v6leasequery field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v6leasequery_reply</td>
<td>Specifies the sum for v6leasequery_reply field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v6rebind</td>
<td>Specifies the sum for v6rebind field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v6reconfigure</td>
<td>Specifies the sum for v6reconfigure field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v6relay_forward</td>
<td>Specifies the sum for v6relay_forward field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v6relay_reply</td>
<td>Specifies the sum for v6relay_reply field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Module</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v6release</td>
<td>Specifies the sum for v6release field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v6renew</td>
<td>Specifies the sum for v6renew field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v6reply</td>
<td>Specifies the sum for v6reply field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v6request</td>
<td>Specifies the sum for v6request field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_v6solicit</td>
<td>Specifies the sum for v6solicit field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_v</td>
<td>Here, v = version. This is not scoped to a single field.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_dhcp_usage_trend, si_dhcp_top_os_by_network, and si-search-dhcp-message</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_FREE_ADDRESSES</td>
<td>Contains precision of the FREE_ADDRESSES field</td>
<td>si_dhcp_usage_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_dhcp_utilization</td>
<td>Contains precision of the dhcp_utilization field</td>
<td>si_dhcp_range_utilization_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_dynamic_hosts</td>
<td>Contains precision of the dynamic_hosts field</td>
<td>si_dhcp_usage_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_static_hosts</td>
<td>Contains precision of the static_hosts field</td>
<td>si_dhcp_usage_trend</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v4ack</td>
<td>Contains precision of the v4ack field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v4decline</td>
<td>Contains precision of the v4decline field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v4discover</td>
<td>Contains precision of the v4discover field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v4inform</td>
<td>Contains precision of the v4inform field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v4leaseactive</td>
<td>Contains precision of the v4leaseactive field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v4leasequery</td>
<td>Contains precision of the v4leasequery field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v4leaseunassigned</td>
<td>Contains precision of the v4leaseunassigned field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v4leaseunknown</td>
<td>Contains precision of the v4leaseunknown field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v4nak</td>
<td>Contains precision of the v4nak field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v4offer</td>
<td>Contains precision of the v4offer field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v4release</td>
<td>Contains precision of the v4release field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v4request</td>
<td>Contains precision of the v4request field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v6advertise</td>
<td>Contains precision of the v6advertise field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v6confirm</td>
<td>Contains precision of the v6confirm field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v6decline</td>
<td>Contains precision of the v6decline field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v6information_request</td>
<td>Contains precision of the v6information_request field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_v6leasequery</td>
<td>Contains precision of the v6leasequery field</td>
<td>si-search-dhcp-message</td>
<td></td>
</tr>
<tr>
<td>Extracted Field Name</td>
<td>Description of the field</td>
<td>Reports</td>
<td>Values/Range</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------</td>
<td>---------</td>
<td>--------------</td>
</tr>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_max_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_min_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_search_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitor</td>
<td>Specifies the monitor String. Example: https</td>
<td></td>
<td></td>
</tr>
<tr>
<td>orig_host</td>
<td>Specifies the host name of the data source Example: infoblox.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pool</td>
<td>Specifies the Pool String. Example: Pool</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_available</td>
<td>Specifies the count information for available field si_adns_resource_pool_availability and si_smart_dns_resource_availability Splunk added special field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_ct_response_count</td>
<td>Specifies the count information for response_count field</td>
<td>si_dtc_response_distribution</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------</td>
<td>------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>psrsvd_ct_unavailable</td>
<td>Specifies the count information for unavailable field</td>
<td>si_adns_resource_pool_availability and si_smart_dns_resource_availability</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrscd_ct_value</td>
<td>Specifies the count information for value field</td>
<td>si_smart_dns_resource_snmp</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_gc</td>
<td>Here, gc = group count. This is the count for stats grouping and it is not scoped to a single field.</td>
<td>si_dtc_response_distribution, si_smart_dns_resource_snmp, si_adns_resource_pool_availability and si_smart_dns_resource_availability</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_nc_available</td>
<td>Specifies the numerical count information for available field</td>
<td>si_adns_resource_pool_availability and si_smart_dns_resource_availability</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_nc_response_count</td>
<td>Specifies the numerical count information for response_count field</td>
<td>si_dtc_response_distribution</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_nc_unavailable</td>
<td>Specifies the numerical count information for unavailable field</td>
<td>si_adns_resource_pool_availability and si_smart_dns_resource_availability</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_nc_value</td>
<td>Specifies the numerical count information for value field</td>
<td>si_smart_dns_resource_snmp</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_sm_available</td>
<td>Specifies the sum information for available field</td>
<td>si_adns_resource_pool_availability and si_smart_dns_resource_availability</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_sm_response_count</td>
<td>Specifies the sum information for response_count field</td>
<td>si_dtc_response_distribution</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_sm_unavailable</td>
<td>Specifies the sum information for unavailable field</td>
<td>si_adns_resource_pool_availability and si_smart_dns_resource_availability</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_sm_value</td>
<td>Specifies the sum information for value field</td>
<td>si_smart_dns_resource_snmp</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_v</td>
<td>Here, v = version. This is not scoped to a single field.</td>
<td>si_dtc_response_distribution, si_smart_dns_resource_snmp, si_adns_resource_pool_availability and si_smart_dns_resource_availability</td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Splunk added special field</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_available</td>
<td>Contains precision of the available field</td>
<td>Splunk added special field</td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_adns_resource_pool_availability and si_smart_dns_resource_availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_response_count</td>
<td>Contains precision of the response_count field</td>
<td>Splunk added special field</td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_dtc_response_distribution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_unavailable</td>
<td>Contains precision of the unavailable field</td>
<td>Splunk added special field</td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_adns_resource_pool_availability and si_smart_dns_resource_availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_value</td>
<td>Contains precision of the value field</td>
<td>Splunk added special field</td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_smart_dns_resource_snmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>report</td>
<td>Name of the report that populates the summary index</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>si_dtc_response_distribution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Traffic Control</td>
<td>Name of the report that populates the summary index</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource Pool</td>
<td>si_adns_resource_pool_availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability reports</td>
<td>si_smart_dns_resource_snmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Traffic Control</td>
<td>Name of the report that populates the summary index</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource SNMP</td>
<td>si_smart_dns_resource_availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>reports data</td>
<td>si_smart_dns_resource_snmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>resource</td>
<td>Specifies the resource</td>
<td>Infoblox DTC summary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>String. Example: Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>search_name</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>search_now</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>source</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sourcetype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeendpos</td>
<td>Common extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timestartpos</td>
<td>Common extracted fields</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Infoblox System Summary

<table>
<thead>
<tr>
<th>Extracted Field Name</th>
<th>Description of the field</th>
<th>Reports</th>
<th>Values/Range</th>
<th>Source of Data</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER</td>
<td>Specifies the member String. Example: infoblox.localdomain: inbound</td>
<td></td>
<td></td>
<td></td>
<td>Evaluated from host and sys_report_id field values</td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_max_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_min_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_search_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>linecount</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>orig_host</td>
<td>Specifies the host name of the data source</td>
<td>Example: infoblox.com</td>
<td></td>
<td></td>
<td>Splunk added default field</td>
</tr>
<tr>
<td>psrsvd_ct_CPU_PERCENT</td>
<td>Specifies the count information for the CPU_PERCENT field</td>
<td>si_cpu_usage</td>
<td></td>
<td></td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_ct_MEMORY_PERCENT</td>
<td>Specifies the count information for the MEMORY_PERCENT field</td>
<td>si_memory_utilization</td>
<td></td>
<td></td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_ct_TRAF_VALUE</td>
<td>Specifies the count information for TRAF_VALUE field</td>
<td>si_traffic_rate</td>
<td></td>
<td></td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>psrsvd_gc</td>
<td>Here, gc = group count. This is the count for a stats grouping and it is not scoped to a single field.</td>
<td>si_memory_utilization, si_traffic_rate, and si_cpu_usage</td>
<td></td>
<td></td>
<td>Splunk added special field</td>
</tr>
<tr>
<td>Extracted Field Name</td>
<td>Description of the field</td>
<td>Reports</td>
<td>Values/Range</td>
<td>Source of Data</td>
<td>Remarks</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------</td>
<td>---------</td>
<td>--------------</td>
<td>----------------</td>
<td>---------</td>
</tr>
<tr>
<td>psrsvd_nc_CPU_PERCENT</td>
<td>Specifies the numerical count information for CPU_PERCENT field</td>
<td>si_cpu_usage</td>
<td>Splunk added special field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_MEMORY_PERCENT</td>
<td>Specifies the numerical count information for MEMORY_PERCENT field</td>
<td>si_memory_utilization</td>
<td>Splunk added special field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_nc_TRAF_VALUE</td>
<td>Specifies the numerical count information for TRAF_VALUE field</td>
<td>si_traffic_rate</td>
<td>Splunk added special field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_CPU_PERCENT</td>
<td>Specifies the sum for CPU_PERCENT field</td>
<td>si_cpu_usage</td>
<td>Splunk added special field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_MEMORY_PERCENT</td>
<td>Specifies the sum for MEMORY_PERCENT field</td>
<td>si_memory_utilization</td>
<td>Splunk added special field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_sm_TRAF_VALUE</td>
<td>Specifies the sum for TRAF_VALUE field</td>
<td>si_traffic_rate</td>
<td>Splunk added special field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_v</td>
<td>Here, v = version. This is not scoped to a single field.</td>
<td>si_memory_utilization, si_traffic_rate, and si_cpu_usage</td>
<td>Splunk added special field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_CPU_PERCENT</td>
<td>Contains precision of the CPU_PERCENT field</td>
<td>si_cpu_usage</td>
<td>Splunk added special field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_MEMORY_PERCENT</td>
<td>Contains precision of the MEMORY_PERCENT field</td>
<td>si_memory_utilization</td>
<td>Splunk added special field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>psrsvd_vt_TRAF_VALUE</td>
<td>Contains precision of the TRAF_VALUE field</td>
<td>si_traffic_rate</td>
<td>Splunk added special field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>report</td>
<td>Specifies the name of the report that is populating the summary index</td>
<td>si_index_disk_usage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Index Disk Usage Report Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory Utilization Trend data</td>
<td>si_memory_utilization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Traffic Rate by Member report data</td>
<td>si_traffic_rate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CPU Utilization Trend data</td>
<td>si_cpu_usage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search_name</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search_now</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>source</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sourcetype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>splunk_server_group</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeendpos</td>
<td>Common extracted fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timestartpos</td>
<td>Common extracted fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Infoblox Security Summary**

*Copyright ©2019, Infoblox, Inc. All right reserved.*
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Type</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTIVE_COUNT</td>
<td>Specifies the active count</td>
<td>Integer</td>
<td>Infoblox security summary</td>
</tr>
<tr>
<td>BLOCK_END</td>
<td>Specifies the block end IP address</td>
<td>Integer</td>
<td>Infoblox security summary</td>
</tr>
<tr>
<td>BLOCK_START</td>
<td>Specifies the block start IP address</td>
<td>Integer</td>
<td>Infoblox security summary</td>
</tr>
<tr>
<td>DNST_CATEGORY</td>
<td>Specifies the destination category</td>
<td>String</td>
<td>atp_rule_sid_lookup lookup from /tmp/reporting_atp_conf/atp_rule_sid_lookup.csv with RULE_SID value as input</td>
</tr>
<tr>
<td>EA</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HWTYPE</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DB_OBJECTS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DHCP_LPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAX_DNS_QPS</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEMBER_IP</td>
<td>Common Extracted fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAT_STATUS</td>
<td>Specifies the NAT status</td>
<td>String</td>
<td>Infoblox security summary</td>
</tr>
<tr>
<td>RULE_DESCRIPTION</td>
<td>Specifies the rule description</td>
<td>String</td>
<td>atp_rule_sid_lookup lookup from /tmp/reporting_atp_conf/atp_rule_sid_lookup.csv with RULE_SID value as input</td>
</tr>
<tr>
<td>RULE_NAME</td>
<td>Specifies the rule name</td>
<td>String</td>
<td>atp_rule_sid_lookup lookup from /tmp/reporting_atp_conf/atp_rule_sid_lookup.csv with RULE_SID value as input</td>
</tr>
<tr>
<td>RULE_SID</td>
<td>Specifies the rule SID</td>
<td>Integer</td>
<td>Infoblox security summary</td>
</tr>
<tr>
<td>SOURCE_IP</td>
<td>Specifies the source IP</td>
<td>IP address</td>
<td>Infoblox security summary</td>
</tr>
<tr>
<td>SOURCE_PORT</td>
<td>Specifies the source port</td>
<td>Integer</td>
<td>Infoblox security summary</td>
</tr>
<tr>
<td>date_hour</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_mday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_minute</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_month</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_second</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_wday</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_year</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>date_zone</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eventtype</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>index</td>
<td>Splunk Default field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_max_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>info_min_time</td>
<td>Common summary index fields</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### When to Update?

You must update this document in the following scenarios of the reporting data model:

- When new indexes are introduced.
- When new fields are added to or deleted from existing indexes.
- Cron schedules of existing summary indexes are modified.
- Cron schedules are added for a new summary.

### How to Update?

Please read the following before you update this document:

1. Populate the required index with data in the Grid setup.
2. Use the following command to get a list of all fields within each index:
   ```shell
   index=ib_xxxx | fieldsummary
   ```
3. Add those lists of fields to the table in the index.
4. Determine sample field values from search results.
5. Manually figure out the source data path of each field.

For existing fields go through:

- `default/props.conf`
- `default/transforms.conf`
- `default/savedsearches.conf` configuration files from IBRA code
- `products/reporting/server/src/pyutil/reporting_config_writer_util.py` from NIOS code.

The following path is commonly found for file based (like .csv, .txt, .log) extractions in each forwarder: `/infoblox/var/reporting/
Lookup files path in an indexer: `/storage/splunk/etc/apps/infoblox/lookups/`
Part 8 Infoblox Infrastructure Security

The mission-critical DNS infrastructure can become a vulnerable component in your network when it is inadequately protected by traditional security solutions and consequently used as an attack surface. Compromised DNS services can result in catastrophic network and system failures. To fully protect your network in today's cyber security threat environment, Infoblox sets a new DNS security standard by offering scalable, enterprise-grade, and integrated protection for your DNS infrastructure.

While your external (internet-facing) DNS server can be subject to cyber attacks such as DNS DDoS (Distributed Denial of Service) and others, threats can also come from the inside of your firewalls. Today's targeted attacks pose risk to both data and infrastructure inside an enterprise. You could have an endpoint infected with malware or threats trying to communicate with C&C (Command-and-Control) servers that use DNS as a protocol. You could also have a malicious insider trying to steal valuable digital assets by opening a DNS tunnel or embedding data in DNS queries.

Depending on how you want to protect your mission-critical DNS infrastructure, you can configure your Infoblox appliance to mitigate against external, internal, or both (external and internal) DNS threats. This section contains information about the Infoblox infrastructure security features that protect external DNS from cyber DNS attacks and internal DNS from infrastructure attacks, data exfiltration, and APTs (Advanced Persistent Threats) and malware.

- **Infoblox Advanced DNS Protection**

  The Infoblox Advanced DNS Protection solution employs hardware-accelerated security rules to detect, report upon, and stop attacks such as DDoS, DNS reflection, DNS amplification, DNS hijacking, and other network attacks targeting DNS authoritative applications. This security solution helps minimize "false positives" and ensures that your mission-critical DNS services continue to function even when under attack. For more information, see [Infoblox Advanced DNS Protection](#).

- **Infoblox DNS Firewall**

  Infoblox DNS Firewall uses DNS RPZs (Response Policy Zones) for allowing reputable sources to dynamically communicate reputation domain names so you can implement policy controls for DNS lookups. For more information, see [Infoblox DNS Firewall](#).

- **Infoblox Threat Insight**

  The Infoblox Threat Insight solution defends against data exfiltration through DNS tunneling for ultimate network protection. For more information, see [Infoblox Threat Insight](#).

- **Security Ecosystem**

  The Infoblox security ecosystem comprises FireEye integrated RPZs for detecting malware and APTs and the TAXII (Trusted Automated eXchange of Indicator Information) service for mitigating cyber attacks. For more information, see [Infoblox DNS Firewall](#).

  For best practices in securing your networks, you can also set up DNS blacklists or configure a security banner. When you enable DNS Integrity Check for top-level authoritative zones, the appliance verifies DNS data in the NS RRsets and glue records, and reports any data discrepancies so you can mitigate possible DNS domain hijacking.

  Following are other DNS security features for your network security:

  - **Access Control (Named ACLs)**

    To effectively manage your core network services, you can grant legitimate hosts access to specific operations on the appliance using an ACL (access control list) or anonymous ACEs (access control entries). You can also configure a named ACL and apply it to multiple operations, such as file distribution and DNS zone transfers. For more information, see [Configuring Access Control](#).

  - **DNS blacklists**

    Your organization can prevent customers or employees from accessing certain Internet resources, particularly web sites, by prohibiting a recursive DNS member from resolving queries for domain names that you specify. You can configure a recursive DNS member to redirect the DNS client to predefined IP addresses or return a REFUSED response code (indicating that resolution is not performed because of local policy), depending on the domain name. For more information, see [About Blacklists](#).

  - **Security Banner**

    You can configure and publish a notice and consent banner as the first login screen that includes specific terms and conditions you want end users to accept before they log in to the Infoblox Grid. When you enable the notice and consent banner, users must accept the terms and conditions displayed on the consent screen before accessing the login screen of Grid Manager. For more information, see [Configuring Notice and Consent Banner](#).

  - **DNS Integrity Check**

    DNS domain hijacking or domain theft is the act of changing the registration of a domain name without the permission of its original registrant. In some cases, hijackers change the DNS data of a domain after gaining control of it. They consequently redirect users to a fraudulent site, instead
of the legitimate site, on the Internet. To protect your authoritative DNS servers against this type of domain hijacking, you can configure the appliance to monitor NS records and glue records for top-level authoritative zones. Based on your configuration, the appliance periodically checks the DNS data for the zones and compares the data with that in the appliance database. The severity in data discrepancies can help identify possible domain hijacking. For more information about this feature, see About DNS Integrity Check for Authoritative Zones.

Chapter 41 Infoblox Advanced DNS Protection

This chapter describes the Infoblox Advanced DNS Protection solution and its features. It explains how to enable and disable the threat protection service, define threat protection rule settings, and manage threat protection rules so you can protect your internet-facing authoritative servers. It contains the following sections:

- About Infoblox Advanced DNS Protection
  - Configuring Infoblox Advanced DNS Protection
  - Supported Threat Protection Appliances and Licensing Requirements
  - Administrative Permissions
  - Starting and Stopping Threat Protection Service
  - Enabling and Disabling Monitoring Mode
- Understanding Threat Protection Rulesets and Rules
  - About Ruleset Versions and Updates
  - System and Auto Rules
  - Custom Rules
  - Creating Custom Rules
- Configuring Grid Security Properties
  - Enabling Multiple DNS Requests through a Single TCP Session
  - Configuring NAT Mapping Properties
- Managing Threat Protection Rulesets
  - Viewing Threat Protection Rulesets
  - Activating a Ruleset
  - Overriding the Grid Ruleset
  - Modifying Rulesets
  - Comparing and Merging Rulesets
  - Manually Uploading Rulesets
  - Publishing Rule Updates
- Configuring Threat Protection Profiles
  - Adding Threat Protection Profiles
  - Cloning Threat Protection Profiles
  - Modifying Threat Protection Profiles
  - Merging Threat Protection Profiles
  - Inheriting Grid Rule Settings
  - Deleting Threat Protection Profiles
  - Viewing Threat Protection Profiles
- Managing Threat Protection Rules
  - Viewing Threat Protection Rules
  - Enabling and Disabling Rules
  - Modifying System and Auto Rules
  - Publishing Rule Updates
  - Modifying System and Auto Rules
  - Modifying Custom Rules
  - Monitoring Threat Protection Events
- Monitoring Threat Protection Events
  - Monitoring through Syslog
  - Threat Protection Statistics Widget
  - Threat Protection Reports
- DNS and Network-Flood Threats
  - Internet Control Message Protocol (ICMP) Flood
  - SYN Flood
  - UDP DNS Flood
  - Inside-Out Attacks
  - DNS Fluxing
  - DNS Cache Poisoning
  - DNS Reflection and Amplification Attacks
  - DNS Malware
  - DNS Domain Hijacking

About Infoblox Advanced DNS Protection

The Infoblox Advanced DNS Protection solution employs threat protection rules to detect, report upon, and stop DoS (Denial of Service), DDoS (Distributed Denial of Service) and other network attacks targeting DNS authoritative applications. Infoblox Advanced DNS Protection helps
minimize "false positives" and ensures that your mission-critical DNS services continue to function even when under attack. For information about possible DNS threats, see DNS and Network-Flood Threats.

You can deploy the Advanced DNS Protection solution on hardware-accelerated appliances (physical appliances only) as well as software-based appliances (both physical and virtual) in the Grid. Depending on the appliances you deploy, you must install applicable hardware-based licenses or Software ADP subscription licenses. For information about supported Infoblox appliances for Advanced DNS Protection and the applicable licenses, see Supported Threat Protection Appliances and Licensing Requirements.

Infoblox Advanced DNS Protection is designed to provide visibility and protection against network floods and DNS attacks. It detects DNS attacks through predefined and custom threat protection rules, and mitigates DNS threats by dropping problematic packets while responding only to legitimate traffic. With valid licenses installed, you can subscribe to automatic rule updates that deliver near real-time protection against new and emerging attacks. You may also manually perform the rule update process based on your configuration. For information about threat protection rules, see Understanding Threat Protection Rulesets and Rules.

Infoblox Advanced DNS Protection supports a set of predefined threat protection rules that detect and mitigate possible DNS threats. You can modify some of the parameters and assign actions such as logging events and applying mitigation to these rules. You can also create custom rules to suit your security needs. For more information, see Understanding Threat Protection Rulesets and Rules.

As illustrated in Figure 43.1, the threat protection appliance, acting as an authoritative DNS server, is added to the Grid. After installing valid threat protection licenses and configuring the appliance to serve as an Advance Appliance, it can now detect DNS threats and mitigate DNS threats based on threat protection rules. All threat protection related events, conformed to CEF (Common Event Format), are logged in the syslog on the Grid Master. To perform further investigation about possible threats, the reporting server generates specific threat protection related reports. For information about how to monitor threat protection related events and reports, see Monitoring Threat Protection Events.

**Figure 41.1 Infoblox Advanced DNS Protection Solution**

Limitations for Threat Protection Appliances

Hardware-based appliances support all existing DNS features (including HA support) that are applicable to DNS caching and authoritative applications, except the following:

- Configuration of multiple interfaces on the same subnet
- 10/100-Mbps gigabit Ethernet mode and fixed speed/duplex settings

**Note:** Even though you can configure static routes on the Infoblox-4030 Rev-2 appliance when DNS cache acceleration is enabled, cached DNS responses are always sent through the interface on which the queries arrive, not the interface that is configured for the static route.

Consider the following when the threat protection service is enabled on the Advance Appliances:

**For Hardware ADP**

- Protected interfaces (LAN1 and LAN2) are limited to DNS traffic, protocols in support of DNS anycast (BGP and OSPF) and the standard IP protocols such as ICMP, as well as connections to NTP servers.
- The MGMT interface is used for other traffic, such as Grid, SSH, SNMP, NTP, and it will not be protected against DDoS attacks.
- You cannot run other services, such as FTP, TFTP, and HTTP, on the Advance Appliances.
- The appliance terminates TCP connections for incoming DNS requests after handling the initial request through each TCP connection.
The exception for this default Grid setting is for an SOA query sent by a client that is accepted in the allow-transfer ACL. In the case of an SOA query, the TCP connection remains open for subsequent DNS requests. This exception also covers the case in which an AXFR query follows the SOA query through the same TCP connection. For more information about how to override this default Grid setting, see Enabling Multiple DNS Requests through a Single TCP Session.

For Software ADP

- When you use IB-FLEX for Software ADP, it supports a standalone or a Grid member with threat protection enabled, but it does not support a Grid Master with threat protection enabled. For more information about the IB-FLEX virtual appliance model, see About IB-FLEX X.
- IB-FLEX applies threat protection rules to all traffic on LAN1, LAN2 and HA interfaces, but bypasses the traffic on the MGMT interface.
- The threat protection profiles used for Software ADP members do not support ADP NAT settings. For more information, see Configuring Threat Protection Profiles. However, you can configure them for hardware-based threat protection members in the Member Security properties editor. For more information, see Configuring Grid Security Properties.

Chapter 42 Infoblox Advanced DNS Protection

This chapter describes the Infoblox Advanced DNS Protection solution and its features. It explains how to enable and disable the threat protection service, define threat protection rule settings, and manage threat protection rules so you can protect your internet-facing authoritative servers. It contains the following sections:

- About Infoblox Advanced DNS Protection
  - Configuring Infoblox Advanced DNS Protection
  - Supported Threat Protection Appliances and Licensing Requirements
  - Administrative Permissions
  - Starting and Stopping Threat Protection Service
  - Enabling and Disabling Monitoring Mode
- Understanding Threat Protection Rulesets and Rules
  - About Ruleset Versions and Updates
  - System and Auto Rules
  - Custom Rules
  - Creating Custom Rules
- Configuring Grid Security Properties
  - Enabling Multiple DNS Requests through a Single TCP Session
  - Configuring NAT Mapping Properties
- Managing Threat Protection Rulesets
  - Viewing Threat Protection Rulesets
  - Activating a Ruleset
  - Overriding the Grid Ruleset
  - Modifying Rulesets
  - Comparing and Merging Rulesets
  - Manually Uploading Rulesets
  - Publishing Rule Updates
- Configuring Threat Protection Profiles
  - Adding Threat Protection Profiles
  - Cloning Threat Protection Profiles
  - Modifying Threat Protection Profiles
  - Merging Threat Protection Profiles
  - Inheriting Grid Rule Settings
  - Deleting Threat Protection Profiles
  - Viewing Threat Protection Profiles
- Managing Threat Protection Rules
  - Viewing Threat Protection Rules
  - Enabling and Disabling Rules
  - Modifying System and Auto Rules
  - Publishing Rule Updates
  - Modifying System and Auto Rules
  - Modifying Custom Rules
  - Monitoring Threat Protection Events
- Monitoring Threat Protection Events
  - Monitoring through Syslog
  - Threat Protection Statistics Widget
  - Threat Protection Reports
- DNS and Network-Flood Threats
  - Internet Control Message Protocol (ICMP) Flood
  - SYN Flood
  - UDP DNS Flood
  - Inside-Out Attacks
  - DNS Fluxing
About Infoblox Advanced DNS Protection

The Infoblox Advanced DNS Protection solution employs threat protection rules to detect, report upon, and stop DoS (Denial of Service), DDoS (Distributed Denial of Service) and other network attacks targeting DNS authoritative applications. Infoblox Advanced DNS Protection helps minimize "false positives" and ensures that your mission-critical DNS services continue to function even when under attack. For information about possible DNS threats, see DNS and Network-Flood Threats.

You can deploy the Advanced DNS Protection solution on hardware-accelerated appliances (physical appliances only) as well as software-based appliances (both physical and virtual) in the Grid. Depending on the appliances you deploy, you must install applicable hardware-based licenses or Software ADP subscription licenses. For information about supported Infoblox appliances for Advanced DNS Protection and the applicable licenses, see Supported Threat Protection Appliances and Licensing Requirements.

Infoblox Advanced DNS Protection is designed to provide visibility and protection against network floods and DNS attacks. It detects DNS attacks through predefined and custom threat protection rules, and mitigates DNS threats by dropping problematic packets while responding only to legitimate traffic. With valid licenses installed, you can subscribe to automatic rule updates that deliver near real-time protection against new and emerging attacks. You may also manually perform the rule update process based on your configuration. For information about threat protection rules, see Understanding Threat Protection Rulesets and Rules.

As illustrated in Figure 41.1, the threat protection appliance, acting as an authoritative DNS server, is added to the Grid. After installing valid threat protection licenses and configuring the appliance to serve as an Advance Appliance, it can now detect DNS threats and mitigate DNS threats based on threat protection rules. All threat protection related events, conformed to CEF (Common Event Format), are logged in the syslog on the Grid Master. To perform further investigation about possible threats, the reporting server generates specific threat protection related reports. For information about how to monitor threat protection related events and reports, see Monitoring Threat Protection Events.

Limitations for Threat Protection Appliances

Hardware-based appliances support all existing DNS features (including HA support) that are applicable to DNS caching and authoritative applications, except the following:

- Configuration of multiple interfaces on the same subnet
- 10/100-Mbps gigabit Ethernet mode and fixed speed/duplex settings

Note: Even though you can configure static routes on the Infoblox-4030 Rev-2 appliance when DNS cache acceleration is enabled, cached DNS responses are always sent through the interface on which the queries arrive, not the interface that is configured for the static route.
Consider the following when the threat protection service is enabled on the Advance Appliances:

**For Hardware ADP**

- Protected interfaces (LAN1 and LAN2) are limited to DNS traffic, protocols in support of DNS anycast (BGP and OSPF) and the standard IP protocols such as ICMP, as well as connections to NTP servers.
- The MGMT interface is used for other traffic, such as Grid, SSH, SNMP, NTP, and it will not be protected against DDoS attacks.
- You cannot run other services, such as FTP, TFTP, and HTTP, on the Advance Appliances.
- The appliance terminates TCP connections for incoming DNS requests after handling the initial request through each TCP connection. The exception for this default Grid setting is for an SOA query sent by a client that is accepted in the allow-transfer ACL. In the case of an SOA query, the TCP connection remains open for subsequent DNS requests. This exception also covers the case in which an AXFR query follows the SOA query through the same TCP connection. For more information about how to override this default Grid setting, see *Enabling Multiple DNS Requests through a Single TCP Session*.

**For Software ADP**

- When you use IB-FLEX for Software ADP, it supports a standalone or a Grid member with threat protection enabled, but it does not support a Grid Master with threat protection enabled. For more information about the IB-FLEX virtual appliance model, see *About IB-FLEX*.
- IB-FLEX applies threat protection rules to all traffic on LAN1, LAN2 and HA interfaces, but bypasses the traffic on the MGMT interface.
- The threat protection profiles used for Software ADP members do not support ADP NAT settings. For more information, see *Configuring Threat Protection Profiles*. However, you can configure them for hardware-based threat protection members in the Member Security properties editor. For more information, see *Configuring Grid Security Properties*.

**Configuring Infoblox Advanced DNS Protection**

To enable and configure Infoblox Advanced DNS Protection on supported Infoblox appliances, complete the following:

1. Obtain valid Threat Protection, Threat Protection (Software add-on) and Threat Protection Update licenses from Infoblox and install them on the Infoblox Advance Appliances. For information about license requirements, see *Supported Threat Protection Appliances and Licensing Requirements*.
2. Optionally, you can set up an HA pair using the same appliance models for both the active and passive nodes. For information about HA pairs, see *About HA Pairs*. Note that you cannot configure Advance Appliances as an HA Grid Master or HA Grid Master candidate.
3. Enable threat protection service, as described in *Starting and Stopping Threat Protection Service*. For an HA pair, enable the service on both the active and passive nodes.
4. Configure threat protection rule settings for the Grid, including automatic or manual rule updates, as described in *Configuring Grid Security Properties*. If your network configuration requires rule updates to go through a proxy server, you can configure the appliance to use a proxy server to send rule updates. For more information, see *Configuring Proxy Servers*. You can also delegate ruleset updates to specific Grid members and change the default interface to an alternate interface, as described in *Configuring Members and Interfaces for Automatic Updates*. Define threat protection profiles for the Grid or specific members, as described in *Configuring Threat Protection Profiles*.
5. Optionally, you can do the following:
   - Override the default Grid setting that disables multiple DNS requests through one TCP session, as described in *Enabling Multiple DNS Requests through a Single TCP Session*.
   - Modify system rules, as described in *Modifying System and Auto Rules*.
   - Create custom rules using rule templates, as described in *Creating Custom Rules*.

After you have successfully set up Infoblox Advanced DNS Protection, you can do the following:

- View the current threat protection rules, as described in *Viewing Threat Protection Rules*.
- Modify system and custom threat protection rules, as described in *Managing Threat Protection Rules*.
- Manually upload rule updates, as described in *Manually Uploading Rulesets*.
- Publish uploaded rule updates, as described in *Publishing Rule Updates*.
- For manual updates, compare differences between two rulesets and merge parameter changes from an old ruleset into a new one, as described in *Comparing and Merging Rulesets*.
- Set the threat protection service in monitor mode, as described in *Enabling and Disabling Monitoring Mode*.
- Add threat protection profiles, as described in *Adding Threat Protection Profiles*.
- Clone threat protection profiles, as described in *Cloning Threat Protection Profiles*.
- Modify threat protection profiles, as described in *Modifying Threat Protection Profiles*.
- Merge threat protection profiles, as described in *Merging Threat Protection Profiles*.
- Inherit Grid rule settings for a threat protection profile, as described in *Inheriting Grid Rule Settings*.
- Delete a threat protection profile, as described in *Deleting Threat Protection Profiles*.
- View the current threat protection profiles, as described in *Viewing Threat Protection Profiles*.

**Supported Threat Protection Appliances and Licensing Requirements**

The Infoblox Advanced DNS Protection solution offers the following licenses: Threat Protection, Threat Protection (Software add-on), and Threat Protection Update. The following are descriptions for each of these licenses:
• **Threat Protection**: Install this license on the physical or hardware-based threat protection appliances. With valid licenses installed, Infoblox Advanced DNS Protection supports both IPv4 and IPv6. You can configure two appliances of the same model to form an HA pair for high availability configuration. For more information about how to configure an HA pair for Infoblox Advanced DNS Protection and its limitations, see *About HA Pairs*. You can configure hardware-based appliances in either IPv4, IPv6, or dual mode (IPv4 and IPv6) network environment.

**Note**: Reverting to an earlier NIOS release that does not support HA configuration for these appliances could cause a service outage.

• **Threat Protection (Software add-on)**: The Software ADP license is a subscription license. Grid Manager displays a warning message when the license expires. You must renew the license to use the Software ADP service. To renew the license, contact your Infoblox representative or Infoblox Technical Support. Before you obtain your permanent license, you can install a temporary license for Threat Protection (Software add-on) using the `set temp_license` CLI command. For more information, refer to the *Infoblox CLI Guide*. Infoblox supports Threat Protection (Software add-on) and Threat Protection Update licenses for elastic scaling. For more information, see *About Elastic Scaling*.

**Note**: You cannot install Multi-Grid Management and Microsoft Management licenses if you install Threat Protection or Threat Protection (Software add-on) licenses on the NIOS appliance.

• **Threat Protection Update**: To receive initial and subsequent threat protection rules and rule updates, you must have the Threat Protection Update license installed. You can then configure NIOS to automatically download and publish threat protection rules or you can manually complete the process. For information, see *Manually Uploading Rulesets* and *Publishing Rule Updates*.

With valid licenses installed, the threat protection appliance can be used as a DNS caching or DNS authoritative server. You can join the appliance to the Grid and treat it as a Grid member. Note that if you install a Threat Protection license on a member, you can enable threat protection only on this member. Contact your Infoblox representative to obtain the Threat Protection, Threat Protection Update and Threat Protection (Software add-on) licenses. For information about licenses, see *Managing Licenses*.

The following table lists all the supported threat protection appliance models and licenses that you can install on them to activate threat protection:

### Table 41.1 Threat Protection Appliance Models and Appliances

<table>
<thead>
<tr>
<th>Threat Protection Appliance Model</th>
<th>Physical or Virtual</th>
<th>Required License</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infoblox-4030 Rev-2</td>
<td>Physical</td>
<td>Threat Protection and Threat Protection Update</td>
<td>DNS Cache Accelerator Appliance</td>
</tr>
<tr>
<td>Infoblox-4030-10GE</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PT-1400</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PT-1405</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PT-2200</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PT-2205</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PT-2205-10GE</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PT-4000</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PT-4000-10GE</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE-815</td>
<td>Physical</td>
<td>Threat Protection (Software add-on) and Threat Protection Update</td>
<td>Trinzic appliances</td>
</tr>
<tr>
<td>TE-825</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE-1410</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE-1415</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE-1420</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE-V815</td>
<td>Virtual</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE-V825</td>
<td>Virtual</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE-V1410</td>
<td>Virtual</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE-V1415</td>
<td>Virtual</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE-V1420</td>
<td>Virtual</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE-V4015</td>
<td>Virtual</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IB-FLEX</td>
<td>Virtual</td>
<td>Threat Protection (Software add-on) and Threat Protection Update</td>
<td>IB-FLEX</td>
</tr>
</tbody>
</table>

You can install the Threat Protection (Software add-on) license on the following hypervisors:
For more information about these appliances, refer to the respective installation guides under the Tech Docs tab on the Infoblox Support site at https://support.infoblox.com.

Administrative Permissions

Superusers can configure all threat protection related tasks. You can assign Security Permissions to specific admin groups and roles. You can also add a global permission for managing Grid security properties or add an object permission for managing member security properties. To perform any action on the rulesets and rules, you must have a Read-write permission for Grid Security properties and Member Security properties at the Grid level and the member level respectively. For more information about security permissions, see Administrative Permissions for DNS Threat Protection.

Starting and Stopping Threat Protection Service

After you install the Threat Protection licenses on the appliance, you can start the threat protection service so you can monitor and mitigate DNS threats on that appliance.

To start or stop threat protection service:

1. From the Grid tab, select the Grid Manager tab -> Services tab, click the Threat Protection service link, and then select the member check box.
2. From the Toolbar, click Start to start the service or Stop to stop the service.

Note that when you stop threat protection service, the appliance does not provide visibility or protection against network floods or DNS threats. After you enable threat protection service, you can configure rule settings, add custom rules, and evaluate system rules to ensure that mitigation to DNS threats is handled properly. You can also temporary disable the threat protection service when necessary. For information about how to configure Grid security settings, see Configuring Grid Security Properties.

Note: Starting and stopping threat protection service on the Infoblox-4030 Rev-2 appliance may trigger a product restart.

Note that under normal circumstances when the system is not experiencing any attack, enabling the threat protection service may have a significant performance impact. When the system is under attack, enabling the threat protection service may have a higher performance impact. You might also notice a significant increase in the memory usage due to the threat protection service. You cannot replicate Grid, member, and profile level threat protection configuration changes during a scheduled full upgrade.

Enabling and Disabling Monitoring Mode

To ensure that blocking certain DNS queries and packets through threat protection rules does not cause unintended effect on your appliance, you can set the threat protection service in monitor mode. You can also put your appliance in this mode to rule out the possibility that the DNS server is dropping DNS queries. When monitor mode is enabled, the appliance logs DNS packets (instead of dropping them) that would have been blocked by threat protection rules. This information is recorded in the syslog.

When the Threat Protection service is in monitor mode, the service status changes from Threat Protection Service is working to Threat Protection is working in monitor mode and the status color changes from green to yellow. The status appears in both the Data Management tab -> Security tab -> Members tab and in the Grid tab -> Grid Manager tab -> Services tab. Note that when one of the members is in monitor mode, the overall status for the Threat Protection service changes from green to yellow. For more information about viewing service status, see Monitoring Services.

You can enable or disable the monitor mode for individual Grid members through the CLI command set smartnic monitor-mode. You cannot set this configuration at the Grid level. To enable or disable monitor mode for both hardware and Software ADP profiles, you can use the command set adp monitor-mode on/off. The show adp command displays the status of the monitor mode. Grid Manager displays a warning if the threat protection profile is running in monitor mode.

For more information about this command, refer to the Infoblox CLI Guide. Note that the set smartnic monitor-mode command is recorded in the audit log while the threat protection events are recorded in the syslog. For information about the audit log and syslog, see Monitoring Tools.

Understanding Threat Protection Rulesets and Rules

To fully implement Infoblox Advanced DNS Protection, ensure that you import the latest threat protection ruleset. To import rulesets, you must have the Threat Protection Update license installed on the appliance. For more information, see Supported Threat Protection Appliances and Licensing Requirements. A ruleset comprises all threat protection rules, including system and auto-generated rules, rule templates, custom rules (if any), and parameter definitions and values. For detailed information about threat protection rules, refer to the Infoblox Threat Protection Rules available on the Support site. Infoblox supports a common threat protection ruleset for both hardware and Software ADP members. This ruleset supports all rules and templates. You can also manually upload your rulesets or download rulesets automatically from the IT server.

Infoblox Advanced DNS Protection supports the following threat protection rules:

- Predefined system and auto-generated rules, as described in System and Auto Rules.
- Custom rules, as described in Custom Rules.

Each threat protection rule belongs to a rule category. When you import a ruleset, the appliance publishes the system and auto rules in their respective categories. NIOS automatically manages rule categories and you cannot add, delete, or modify them. It also provides rule templates for creating custom rules. During a ruleset update, some categories and rules may be added or removed. These actions are performed without
You can recover only custom rules from the Recycle Bin, if enabled. Rules, rule templates and categories that are removed through rulesets are permanently deleted and cannot be restored from the Recycle Bin.

To obtain initial rules and subsequent rule updates, you can configure the appliance to automatically download and publish rulesets or you can manually download them from the Infoblox Support web site and then publish them. For information about how to configure automatic and manual rule settings, see Configuring Grid Security Properties. Note that only the Grid Master receives rules and rule updates. Grid member receives rules and updates through standard Grid replication from the Grid Master. Ruleset data is not replicated to Grid members that do not have the Threat Protection services enabled. Infoblox recommends that you configure the appliance to automatically receive ruleset updates so your appliance receives the latest rules periodically. If you prefer to manually download and publish rulesets, ensure that you download them frequently to receive the most updated rules. The appliance can store up to nine ruleset versions, and you can select up to five rulesets and switch between these versions for the Grid or members when necessary. For more information about ruleset versions and updates, see About Ruleset Versions and Updates.

Packet Flow for Threat Protection Rules

Threat protection rules are designed to work together to provide maximum protection for your environment. This section describes how these rules are being applied and how you can tune some of them to suit your system setup and network environment. Threat protection rules are grouped by rule categories, and most of them have one or more associated rule parameters. All threat protection rules contain rule parameters that you may or may not be able to configure. Rule parameters are predefined with default values that generally suit most network environments. However, there are times when you have special setups or configurations in your environment that require special attention. In these cases, you may need to change some of the rule parameters to obtain optimal protection without sacrificing system performance. For detailed information about all threat protection rules and how to tune them when necessary, refer to the Infoblox Threat Protection on Rules available on the Support web site. Depending on the rules, you may or may not be able to override default values for the following rule parameters (when applicable):

- **Packets per second**: This parameter defines the rate limit or the number of packets per second that the appliance processes before it performs a triggered action, such as sending warnings or blocking traffic.
- **Drop interval**: This is the time period (in seconds) for which the appliance blocks traffic from the client or traffic that matches a certain pattern beyond the rate limit. Based on how you want to handle the traffic that exceeds the rate limit, you can configure this interval to work with the **Rate Algorithm** parameter.
- **Rate algorithm**: This parameter defines how the appliance handles incoming traffic when the traffic exceeds the rate limit (defined in **Packets per second**). You can set this to "blocking" or "rate limiting." The default is "rate limiting." When you set this to "blocking," the appliance allows client traffic to go through until it hits the rate limit. It then blocks all traffic for the duration of the drop interval. If client traffic continuously exceeds the rate limit, the appliance continues to block all traffic for subsequent drop intervals without letting through any traffic, which could result in an indefinite traffic blockage. When you set this to "rate limiting," the appliance allows client traffic to go through until traffic hits the rate limit. It then blocks all traffic for the rest of the drop interval. The appliance re-evaluates client traffic at the beginning of each drop interval and repeats the same behavior for subsequent intervals.

To avoid resource exhaustion and limit frauds, you can limit the query rate for each source IP, and then set **Drop interval** to one second and **Rate algorithm** to "rate limiting," which results in a rate-limiting behavior that allows some traffic to go through before the rest of the traffic is blocked. In this case, the appliance re-evaluates the client behavior every second. If the client traffic exceeds the rate limit, the appliance processes only queries up to the rate limit and drops all excessive queries for the remainder of the second.

For more information about how to configure **Rate algorithm**, **Packets per second** and **Drop interval**, see Configuration Examples.

**Note:** Starting with NIOS 6.12.4, the default for **Rate algorithm** has been changed from "blocking" to "rate limiting."

- **Events per second**: The number of events logged per second for the rule. Setting a value to 0 (zero) disables the appliance from logging events for the rule. Most rules have this parameter, and the default value is 1.
- **Packet size**: DNS packet size. If the DNS packet size exceeds a certain value, the corresponding rule will be triggered.

Configuration Examples

Depending on how you want the appliance to handle incoming traffic, you can configure applicable parameters so they work hand-in-hand to deliver desired results. Following are some examples that demonstrate how you can use the **Rate algorithm**, **Packets per second** and **Drop interval** parameters.

**Example 1**

If source IP 100.10.10.1 sends queries at a rate of 100 packets per second, and you have the following configuration for a threat protection rule:

- **Packets per second** = 40
- **Drop interval** = 3
- **Rate algorithm** = blocking

The appliance handles incoming traffic in the following manner:
1st second: 40 packets are allowed; all other packets are blocked
2nd second: All traffic from 100.10.10.1 is blocked
3rd second: All traffic from 100.10.10.1 is blocked
4th second: All traffic from 100.10.10.1 is blocked
5th second: All traffic from 100.10.10.1 is blocked
6th second: All traffic from 100.10.10.1 is blocked

In this example, the appliance evaluates historic data of the client behavior. If the client traffic exceeds the limit, then the appliance continuously drops traffic, which may result in an indefinite traffic blockage for a client that continuously violates the rate limit.

Example 2
Source IP 100.10.10.1 sends queries at a rate of 100 packets per second for a duration of two seconds. It then sends 30 packets per second for three seconds and 50 packets afterwards; and you have the following configuration for a threat protection rule:

- **Packets per second** = 40
- **Drop interval** = 1
- **Rate algorithm** = rate limiting

The appliance handles incoming traffic in the following manner:
1st second: 40 packets are allowed; all other packets are blocked for the remainder of the second
2nd second: 40 packets are allowed; all other packets are blocked for the remainder of the second
3rd second: All traffic from 100.10.10.1 is allowed
4th second: All traffic from 100.10.10.1 is allowed
5th second: All traffic from 100.10.10.1 is allowed
6th second: 40 packets are allowed; all other packets are blocked for the remainder of the second

In this case, the appliance re-evaluates the client behavior every second. If client traffic exceeds the rate limit, the appliance processes queries up to the rate limit and drops all excessive queries for the remainder of the second.

About Ruleset Versions and Updates
Infoblox periodically releases updated rulesets. After an automatic update, the new ruleset is automatically applied to the Grid Master and Grid members that are using the Grid ruleset version. After a manual update, you can manually apply the new ruleset to the Grid and individual Grid members. Before you manually publish a ruleset, you can view differences between the current ruleset and the newly downloaded one. You can also modify some changed parameters and then merge the changes from the old version to the new one. For more information, see Comparing and Merging Rulesets.

You can view the current ruleset version (displayed in the Version column) in one of the following tabs:

- **Grid**: From the Data Management tab, select the Security tab -> Threat Protection Rules tab.
- **Member**: From the Data Management tab, select the Security tab -> Members tab.
- **Profile**: From the Data Management tab, select the Security tab -> Profiles tab.

In a Grid, you can run different versions of rulesets on the Grid Master and Grid members. For example, the Grid Master can use revision 1 and a Grid member can use revision 2 of the ruleset. You can also switch back to a previous ruleset version when necessary, but you cannot change the version number for individual rules.

The appliance retains up to nine (9) rulesets at any given time: five (5) old rulesets, one (1) newly downloaded ruleset and three (3) "Do Not Delete" rulesets. You can configure rulesets as "Do Not Delete" at the Grid level. The appliance retains these rulesets and they cannot be deleted during an automatic or manual ruleset update. To allow a ruleset to be deleted during an update, you must first disable the "Do Not Delete" flag for these rulesets. Note that you cannot delete a ruleset that is used by the Grid or any members. For information about how to configure the "Do Not Delete" flag, see Modifying Rulesets.

For more information about how to add, modify, and delete a ruleset, see Managing Threat Protection Rulesets.

Ruleset Update Behavior
Consider the following behavior during a ruleset update:

- If you have configured the rule update policy as Automatic, the following occurs:
  - For each rule that exists in the current ruleset and is used by a Grid member, the appliance automatically copies all customized

Copyright ©2019, Infoblox, Inc. All right reserved.
parameter values from the current ruleset to the corresponding rules in the new ruleset. For rule templates that exist in the current ruleset and are used by any member in the Grid, the appliance automatically copies the rule instances from the current version to the new ruleset.

- The appliance automatically compares and integrates all rule changes into the new ruleset. For manual ruleset update, you can view the differences between the current ruleset and the newly downloaded ruleset, select specific rules and make modifications to customized parameters, and then merge the changes into the new ruleset before applying it to the Grid and members. For more information about how to view the rule differences and merge changes, see Comparing and Merging Rulesets.
- The new ruleset is applied to the Grid and only members that use the same ruleset version as the Grid through inheritance from the Grid security properties. For members that use the same ruleset version as the Grid but have parameter overrides for certain rules, the overridden values will be copied to the new ruleset.

For information about how to configure the rule update policy, see Configuring Grid Security Properties.

- When there are a total of nine (9) rulesets stored in the database, the ruleset that is not used by the appliance and is not marked as "Do Not Delete" will be replaced by the newly downloaded ruleset.
- If there are more than one ruleset that can be replaced, the appliance selects the oldest version based on the version number.
- If a specific system or auto rule from the current ruleset version does not exist in the new ruleset, it will not be migrated to the new ruleset.
- If a specific template from the current ruleset version does not exist in the new ruleset, all of its custom rules will not be migrate to the new ruleset.

### System and Auto Rules

System rules are predefined threat protection rules that are built into the Advance Appliances. New system rules are added through rule updates. You can enable an entire category of system rules as well as individual rules. Note that you cannot add or delete system rules, though you can change some parameters. For most system rules, you can modify the Action and Log Severity. For more information, see Modifying System and Auto Rules.

Auto-generated rules are firewall rules that are automatically defined by NIOS for blocking traffic for disabled services and ports. They do not support functionality such as rate limiting. These rules can be grouped into different rule categories and are enabled or disabled by default. You cannot enable or disable auto rules in this release of Infoblox Advanced DNS Protection, though you can set log severity and control logging for these rules. Note that auto rules are automatically enabled or disabled and reconfigured based on the current running services and configuration on the appliance.

### System and Auto Rule Categories

The appliance supports the following system and auto rule categories. For detailed descriptions about each system and auto rule, refer to the Threat Protection Rules document available on the Infoblox Support site.

- **BGP**: Contains auto rules that mitigate attacks that target BGP (Border Gateway Protocol) routing parameters, such as invalid attribute lengths or invalid message types.
- **DNS Amplification and Reflection**: Contains system and auto rules that can be used to mitigate the commonly used methods of DDoS attacks. For information about DNS amplification and reflection, see DNS Reflection and Amplification Attacks.
- **DNS Cache Poisoning**: Contains rate limiting rules that assign bandwidth restrictions rules used to mitigate DNS cache poisoning (on UDP and TCP) that is performed by sending a large volume of fake replies to a recursive server, which can result in hundreds or thousands of redirects. For more information about DNS cache poisoning, see DNS Cache Poisoning.
- **DNS Malware**: Contains rules that protect against DNS malware that posts serious threats to the DNS infrastructure. For information about DNS malware threats, see DNS Malware.
- **DNS DDoS**: Contains system rules that are used to mitigate DNS DDoS attacks on your Advance Appliance. These rules rate limits clients that trigger following DNS responses: NXDOMAIN, NXRRSET, and SERVFAIL.
- **DNS Message Type**: Contains DNS system rules that can be used to filter requests that query specific DNS flags in the DNS message header.
- **DNS Protocol Anomalies**: Contains auto rules that address general DNS protocol attacks such as invalid DNS queries.
- **DNS Tunneling**: Contains auto rules that mitigate against DNS tunneling attacks. For more information, see Inside-Out Attacks.
- **Default Drop**: Contains system rules that automatically drop IP packets that use unusual UDP, TCP, and ICMP traffic is detected.
- **General DDoS**: Contains auto rules that address general DDoS (Distributed Denial of Service) attacks such as loopback address spoofing, and UDP or TCP packets that contain the same source and destination addresses.
- **HA Support**: Contains auto rules that are used to pass packets that go through the Virtual Router Redundancy Protocol (VRRP) and Internet Group Management Protocol (IGMP) for HA (High Availability) support.
- **ICMP**: Contains auto rules that mitigate ICMP and ICMPv6 ping attacks. ICMP ping size (for IPv4 and IPv6) for these rules is limited to 792 bytes. For information about ICMP, see Internet Control Message Protocol (ICMP) Flood.
- **NTP**: Contains auto rules that mitigate attacks that target the NTP (Network Time Protocol). These rules include support for NTP requests and responses, NTP IPv4 and IPv6 ACLs (Access Control Lists), and private mode 7 packets.
- **OSPF**: Contains auto rules that mitigate attacks that target OSPF (Open Shortest Path First) routing parameters, such as invalid attribute lengths or invalid message types.
- **Potential DDoS Related Domains**: Contains system rules the appliance uses to blacklist domains that may have been the targets or subjects in NXDOMAIN or DDoS attacks. These rules block all FQDN lookups on UDP for domains that have been observed to be used as targets in DDoS attacks, and they are enabled by default.
- **Reconnaissance**: Contains auto rules that mitigate network reconnaissance attacks, in which unauthorized remote attackers attempt to access networks by exploiting network standards and communications.
- **TCP/UDP Floods**: Contains DNS system rules that are used to mitigate DNS TCP and UDP floods. For information about TCP/UDP
Custom Rules

Based on your security needs, you can define custom rules using predefined rule templates. Custom rules are typically whitelisting or blacklisting rules. You can create up to 500 custom rules for each rule template offered by Infoblox Advanced DNS Protection. The appliance logs a syslog message if there are more than 500 rules for a specific rule category. You can remove some rules in order to create new ones for that category.

Note: Before upgrading from an earlier NIOS release to NIOS 6.11.x, ensure that you have less than 500 custom rules for each template. Otherwise, the upgrade may fail.

You can add or delete custom rules for the Grid only. You cannot add or delete them for members, but you can enable, disable, and modify certain rule parameters at the member level.

When you create custom rules, NIOS automatically generates the rule ID from the template used. Note that custom rules do not support IDNs (Internationalized Domain Names). You must first convert IDNs into punycode before entering the data. For information about how to create custom rules, see Creating Custom Rules.

When you create custom rules, you are essentially creating whitelisting and blacklisting entries that utilize rate limiting to detect suspicious UDP and TCP traffic. Infoblox Advanced DNS Protection supports a series of rule templates for defining new custom rules. For information about rule templates, see Custom Rule Templates.

Whitelisting rules define a list of allowed resources before they are blocked by the configured rate limit settings. They provide for only a selected set of entities to access the protected environment. Examples include company offices and their associated internal network services, which presumably uses access control systems to enforce them. In effect, addresses or networks that do not match the whitelisting entries are automatically blocked.

Blacklisting rules define a list of disallowed resources through FQDN lookups as well as rate limiting. Blacklists typically allow a far broader base of access to many more entities, and cite a list of specific entities or people that do not have access. Otherwise, any devices or users theoretically have access to the protected environment.

For whitelist entries, the matching values are mandatory, in which the IP address or network of the rule is expressly permitted access. Blacklist entries are forbidden, in which the IP address or network of the rule is expressly denied access. In essence, blacklisting is more secure.

Note: You can create DNS-specific blacklists under the Data Management tab → DNS tab. However, you cannot use this blacklist feature as part of DNS threat protection.

Custom Rule Templates

Infoblox Advanced DNS Protection supports a few custom rule templates from which you create new custom rules. Note that when you use a specific rule template to create custom rules, the new rules reside in their respective rule categories. For information about creating custom rules, see Creating Custom Rules.

For each rule you create, you can define the Events per second value to determine the number of events per second that will be logged for the rule. You can also define specific rule parameters for custom rules, as follows:

When you create custom rules that involve FQDN lookups, the appliance automatically verifies the FQDN syntax and format that you enter in the Value field. It properly translates escaped sequences and special characters that are used to represent specific characters in the FQDN. For example, \032 is interpreted as a space (hex 20), and " is interpreted as the double quote (hex 22). The appliance sends an error message when it detects invalid characters in the FQDN.

Note: Custom rules do not support IDNs (Internationalized Domain Names). To use IDNs for custom rules, you must first convert the IDNs into punycode. You can use the IDN Converter from the Toolbar for the conversion.

- **BLACKLIST FQDN lookup TCP**: Use this rule template to create custom rules for blacklisting DNS queries by FQDN lookups on TCP. In the Rule Parameters table, complete the following:
  - **Blacklisted FQDN**: Enter the FQDN that you want the appliance to block over TCP traffic. NIOS supports an exact match or subdomain matches for the FQDN specified in the rule. For example, if "test.com" is specified as a custom rule, NIOS blocks "test.com" or "abc.test.com" but "abctest.com" will not be blocked.

- **BLACKLIST FQDN lookup UDP**: Use this rule template to create custom rules for blacklisting DNS queries by FQDN lookups on UDP. In the Rule Parameters table, complete the following:
  - **Blacklisted FQDN**: Enter the FQDN that you want the appliance to block over UDP traffic. NIOS supports an exact match or subdomain matches for the FQDN specified in the rule. For example, if "test.com" is specified as a custom rule, NIOS blocks "test.com" or "abc.test.com" but "abctest.com" will not be blocked.

- **BLACKLIST IP TCP Drop prior to rate limiting**: Use this rule template to create rules for blocking IPv4 or IPv6 addresses on TCP before the appliance drops the packets based on rate limiting rules you have defined using the BLACKLIST IP TCP Drop prior to rate limiting template. In the Rule Parameters table, complete the following:
  - **Blacklisted IP address/network**: Enter the IPv4 or IPv6 address from which packets sent are dropped before any relevant rate limiting rules take effect. Note that all TCP traffic from the specified IPv4 and IPv6 addresses and networks will be blocked. Enter network addresses in address/CIDR format.

- **BLACKLIST IP UDP Drop prior to rate limiting**: Use this rule template to create rules for blocking IPv4 or IPv6 addresses on UDP before the appliance drops the packets based on rate limiting rules you have defined using the BLACKLIST IP UDP Drop prior to rate limiting template. In the Rule Parameters table, complete the following:
• **Blacklisted IP address/network**: Enter the IPv4 or IPv6 address from which packets sent are dropped before any relevant rate limiting rules take effect. Note that all UDP traffic from the specified IPv4 and IPv6 addresses and networks will be blocked. Enter network addresses in address/CIDR format.

• **RATELIMITED FQDN lookup TCP**: Use this template to create custom rules that contains rate limiting restrictions for blocking DNS queries by FQDN lookups on TCP traffic. In the Rule Parameters table, complete the following:
  - **Packets per second**: Enter the number of packets per second to define the rate limit for this rule. You define this value to control the rate of TCP traffic that consists of DNS lookups for the FQDN defined in this rule. The default is 5.
  - **Drop interval**: Enter the number of seconds for which the appliance drops packets.
  - **Blacklist rate limited FQDN**: Enter the FQDN that is affected by the rate limit value configured for this rule. The appliance drops the packets sent by this FQDN when the TCP traffic of DNS lookups for this FQDN exceeds the configured rate limit value.

• **RATELIMITED FQDN lookup UDP**: Use this rule template to create custom rules that contains rate limiting restrictions for blocking DNS queries by FQDN lookups on UDP traffic. In the Rule Parameters table, complete the following:
  - **Packets per second**: Enter the number of packets per second to define the rate limit for this rule. You define this value to control the rate of UDP traffic that consists of DNS lookups for the FQDN defined in this rule. The default is 5.
  - **Drop interval**: Enter the number of seconds for which the appliance drops packets.
  - **Blacklist rate limited FQDN**: Enter the FQDN that is affected by the rate limit value configured for this rule. The appliance drops the packets sent by this FQDN when the UDP traffic of DNS lookups for this FQDN exceeds the configured rate limit value.

**Note**: Make sure that you enter a valid FQDN. Example: test.com, foo.com, etc. The appliance does not display an error message when you enter an invalid FQDN. However, the Threat Protection dashboard displays a warning message for the invalid FQDNs. For information, see Threat Protection Status for Grid.

• **RATELIMITED IP TCP**: Use this rule template to create custom rules that contains rate limiting restrictions for blacklisting IP addresses on TCP. If there are certain IP addresses that you want to block before its traffic reaches the rate limit restrictions, you can create a rule using the RATELIMITED IP TCP template. In the Rule Parameters table, complete the following:
  - **Packets per second**: Enter the number of packets per second to define the rate limit for this rule. You define this value to control the rate of TCP traffic that consists of DNS lookups for the IP address or network defined in this rule. The default is 5.
  - **Drop interval**: Enter the time interval in seconds the appliance drops IP packets sent by the rate limited IP address or network defined for this rule. The default is 30 seconds.
  - **Rate limited IP address/network**: Enter the IP address or network that is affected by the rate limit value configured for this rule. The appliance drops the packets sent by this IP address based on the drop interval when the TCP traffic of DNS lookups for this IP address exceeds the configured rate limit value.

• **RATELIMITED IP UDP**: Use this rule template to create custom rules that contains rate limiting restrictions for blacklisting IP addresses on UDP. If there are certain IP addresses that you want to block before its traffic reaches the rate limit restrictions, you can create a rule using the RATELIMITED IP UDP template. In the Rule Parameters table, complete the following:
  - **Packets per second**: Enter the number of packets per second to define the rate limit for this rule. You define this value to control the rate of UDP traffic that consists of DNS lookups for the IP address or network defined in this rule. The default is 5.
  - **Drop interval**: Enter the time interval in seconds the appliance drops UDP packets sent by the rate limited IP address or network defined for this rule. The default is 30 seconds.
  - **Rate limited IP address/network**: Enter the IP address or network that is affected by the rate limit value configured for this rule. The appliance drops the packets sent by this IP address based on the drop interval when the TCP traffic of DNS lookups for this IP address exceeds the configured rate limit value.

• **WHITELIST IP TCP Pass prior to rate limiting**: Use this rule template to create custom rules for allowing certain IP addresses on TCP before the appliance drops the packets based on rate limiting rules you have defined using the RATELIMITED IP TCP template. In the Rule Parameters table, complete the following:
  - **Whitelist IP address/network**: Enter the IPv4 or IPv6 address from which packets sent are allowed before any relevant rate limiting rules take effect.

• **WHITELIST IP UDP Pass prior to rate limiting**: Use this rule template to create custom rules for allowing certain IP addresses on UDP before the appliance drops the packets based on rate limiting rules you have defined using the RATELIMITED IP UDP template. In the Rule Parameters table, complete the following:
  - **Whitelist IP address/network**: Enter the IPv4 or IPv6 address from which packets sent are allowed before any relevant rate limiting rules take effect.

• **WHITELIST TCP Domain**: Use this rule template to create custom rules to allow DNS queries by FQDN lookups on TCP. In the Rule Parameters table, complete the following:
  - **Whitelist FQDN**: Enter the FQDN that you want the appliance to allow over TCP traffic. NIOS supports an exact match or subdomain matches for the FQDN specified in the rule. For example, if "test.com" is specified as a custom rule, NIOS blocks "test.com" or "abc.test.com" but "abctest.com" will not be blocked.

• **WHITELIST UDP Domain**: Use this rule template to create custom rules to allow DNS queries by FQDN lookups on UDP. In the Rule Parameters table, complete the following:
  - **Whitelist FQDN**: Enter the FQDN that you want the appliance to allow over UDP traffic. NIOS supports an exact match or subdomain matches for the FQDN specified in the rule. For example, if "test.com" is specified as a custom rule, NIOS blocks "test.com" or "abc.test.com" but "abctest.com" will not be blocked.

• **BLACKLIST TCP FQDN lookup for DNS Message Type**: Use this rule template to create custom rules for blacklisting FQDN lookups on TCP for the specified DNS message type. In the Rule Parameters table, complete the following:
  - **DNS Record Type**: Select the DNS record type from the drop-down list or enter a valid ENUM for the DNS record. You can enter a value between 1 and 65534. The following DNS resource records are not supported by this rule template: MD (3), MF (4), MB (7), MG (8), MR (9), WKS (11), HINFO (13), MINFO (14), IXFR (251), and AXFR (252) record.
  - **Blacklisted FQDN substring**: Enter the FQDN from which the packets received are blocked over TCP for the specified DNS message type.

• **BLACKLIST UDP FQDN lookup for DNS Message Type**: Use this rule template to create custom rules for blacklisting FQDN lookups...
Creating Custom Rules

Infoblox Advanced DNS Protection provides a few rule templates from which you can create custom rules. For information about the list of rule templates that you can use, see Custom Rule Templates.

To create a custom rule:

1. From the Data Management tab, select the Security tab -> Threat Protection Rules tab -> Ruleset link, and then click Add Custom Rule from the Toolbar.

2. In the Add Custom Rule editor, complete the following:
   - Template: From the drop-down list, select the blacklisting or whitelisting rule template from which you want to create the new rule. For more information about the rule templates, see Custom Rule Templates.
   - Description: Displays the description of the rule that you are about to create. You cannot modify this.
   - Comment: Enter comments to describe the new rule.
   - Disable: Select this if you want to keep the new rule disabled for later use.

3. Click Next and complete the following to configure rule parameters:
   - Description: Displays the description of the rule that you are about to create. You cannot modify this.
   - Action: Displays the operation the appliance performs when an event related to this rule occurs. Some rules are restricted to specific actions. For example, the action for all blacklisting rules is set to Drop, where the appliance drops IP packets when such an event occurs. The action for all whitelisting rules is set to Pass, where the appliance passes IP packets when such an event occurs.
   - Log Severity: Select Critical, Major, Warning or Informational. The log severity you select here determine the severity of the message triggered by a match against the rule.

In the Rule Parameters section, do the following:

- **DNS Record Type**: Select the DNS record type from the drop-down list or enter a valid ENUM for the DNS record. You can enter a value between 1 and 65534. The following DNS resource records are not supported by this rule template: MD (3), MF (4), MB (7), MG (8), MR (9), WKS (11), HINFO (13), MINFO (14), IXFR (251), and AXFR (252) record.
- **Blacklisted FQDN substring**: Enter the FQDN from which the packets received are blocked over UDP for the specified DNS message type.
- **Pass TCP DNS Message Types**: Use this rule template to create custom rules to allow TCP DNS packets that contain the specified DNS record type. In the Rule Parameters table, complete the following:
  - **DNS Record Type**: Select the DNS record type from the drop-down list or enter a valid ENUM for the DNS record. You can enter a value between 1 and 65534. The following DNS resource records are not supported by this rule template: MD (3), MF (4), MB (7), MG (8), MR (9), WKS (11), HINFO (13), MINFO (14), IXFR (251), and AXFR (252) record.
- **Pass UDP DNS Message Types**: Use this rule template to create custom rules to allow UDP DNS packets that contain the specified DNS record type. In the Rule Parameters table, complete the following:
  - **DNS Record Type**: Select the DNS record type from the drop-down list or enter a valid ENUM for the DNS record. You can enter a value between 1 and 65534. The following DNS resource records are not supported by this rule template: MD (3), MF (4), MB (7), MG (8), MR (9), WKS (11), HINFO (13), MINFO (14), IXFR (251), and AXFR (252) record.
- **RATE LIMITED TCP DNS Message Type**: Use this rule template to create custom rules that contain rate limiting restrictions for blacklisting TCP DNS packets that contain the specified DNS record type. In the Rule Parameters table, complete the following:
  - **Packets per second**: Enter the number of packets per second to define the rate limit for this rule. You define this value to control the rate of TCP traffic that consists of DNS packets with the DNS record type defined in this rule. The default is 5.
  - **DNS Record Type**: Select the DNS record type from the drop-down list or enter a valid ENUM for the DNS record. You can enter a value between 1 and 65534. The following DNS resource records are not supported by this rule template: MD (3), MF (4), MB (7), MG (8), MR (9), WKS (11), HINFO (13), MINFO (14), IXFR (251), and AXFR (252) record.
  - **Drop interval**: Enter the number of seconds for which the appliance drops packets.
- **RATE LIMITED UDP DNS Message Type**: Use this rule template to create custom rules that contain rate limiting restrictions for blacklisting UDP DNS packets that contain the specified DNS record type. In the Rule Parameters table, complete the following:
  - **Packets per second**: Enter the number of packets per second to define the rate limit for this rule. You define this value to control the rate of UDP traffic that consists of DNS packets with the DNS record type defined in this rule. The default is 5.
  - **DNS Record Type**: Select the DNS record type from the drop-down list or enter a valid ENUM for the DNS record. You can enter a value between 1 and 65534. The following DNS resource records are not supported by this rule template: MD (3), MF (4), MB (7), MG (8), MR (9), WKS (11), HINFO (13), MINFO (14), IXFR (251), and AXFR (252) record.
  - **Drop interval**: Enter the number of seconds for which the appliance drops packets.
alue field. It properly translates escaped sequences and special characters that are used to represent specific characters in the FQDN. For example, ‘\32’ is interpreted as a space (hex 20), and ‘\u’ is interpreted as the double quote (hex 22). The appliance sends an error message when it detects invalid characters in the FQDN.

4. Click Save & Close.

The new rule, with an automatically assigned rule ID, is created and placed in its corresponding rule category.

Using the Events Per Second Rule Setting

The Events per second setting allows for disabling or throttling of event logs for specific threat protection rules.

Setting the Events per second parameter to zero disables logging for that rule. Setting the parameter to any other number enables threat protection logging for that specific rule. For information about how to configure this, see Configuring Grid Security Properties.

Configuring Grid Security Properties

After you have installed valid threat protection licenses, you can configure rule update settings for the Grid. The Grid settings apply to all members in the Grid. You can select to use an existing threat protection ruleset or use a threat protection profile. A threat protection profile defines specific security settings and ruleset that you want to apply to a specific member or a group of members. For more information about rulesets, see Unders toling Threat Protection Rulesets and Rules. For information about threat protection profiles, see Configuring Threat Protection Profiles. You can override only the global Event per second filter (in the Basic tab) and the Disable multiple DNS requests via single TCP session option (in the Advanced tab) in the Member Security Properties editor by selecting a member and clicking Edit.

To configure rule settings for the Grid or an individual member:

1. Grid: From the Data Management tab, select the Security tab, and then click Grid Security Properties from the Toolbar.
2. In the Grid Security Properties editor, select the Threat Protection tab -> Basic tab, and complete the following:
   - **Active Ruleset Version:** To activate and apply a specific ruleset to the Grid, select the ruleset from the drop-down list.
   - **Active Ruleset Comment:** Displays information about the selected ruleset from the Comment field of the ruleset.

In the Threat Protection Rulesets Updates section, define the rule update policy. The appliance automatically performs rule updates by default. You can choose to manually publish rule updates. For information about how to manually publish rule updates, see Manually Uploading Rulesets and Publishing Rule Updates.

   - **Latest Available Ruleset:** Displays the version string of the last published ruleset. This field changes each time when the ruleset is updated.
   - **Last Checked For Updates:** Displays the timestamp and time zone when you manually upload a ruleset file or automatically download the latest rule update file from the Infoblox rule update server. This field changes the timestamp only when there is a change in the ruleset. The appliance does not update this field if there is no change in the ruleset for the manual upload or automatic download.
   - **Rule Update Policy:** Select the rule update policy from the drop-down list to determine whether updates are being applied automatically or manually. When you select Automatic, the appliance automatically switches to the newly downloaded ruleset and publishes the changes when a ruleset update is applied. Select Manual to manually download updated rulesets and publish them. Note that you must have a valid Threat Protection Update license installed in order to perform ruleset updates. For information about how to perform a manual update, see Manually Uploading Rulesets and Publishing Rule Updates.
   - **Enable Automatic Ruleset Downloads:** Select this to enable automatic ruleset downloads. Note that starting with NIOS 8.0.0, ruleset downloads might take longer than previous releases; but there is no functional impact during the downloads.

**Note:** When you select this, ensure that you configure and enable a valid DNS resolver for the Grid in the Grid Properties editor so the appliance can successfully access the updated ruleset file.

If your network environment does not allow direct HTTP or HTTPS communication with the Internet through a firewall from a secure location in which the Grid Master or the standalone appliance resides, you can configure the Advance Appliance to use a proxy server so you can receive automatic threat protection updates through this connection. Configured proxy settings are for the entire Grid. You cannot configure proxy settings for individual members. For information about how to configure proxy servers, see Configuring Proxy Servers.

   - **Test Connection:** Click this to test the connectivity between the Advance Appliance and the server from which you receive the rule update files. Grid Manager displays a message indicating whether the connection is successful.
   - **Download Rules Now:** Click this to immediately download the latest rule update file from the Infoblox rule update server, provided that the connection between the appliance and the server is successful.

In the Schedule section, define the schedule for automatic ruleset downloads. The following options are enabled only when you have selected Enable Automatic Ruleset Downloads:

   - **Default:** Select this to set the default schedule settings for automatic ruleset downloads.
   - **Custom:** Select this to schedule downloads at a later date and time. Click the Calendar icon to select the date and time.

**Note:** When you schedule automatic ruleset downloads, the downloads are performed within 15 minutes before or after the scheduled time. If you have multiple Grid members configured for downloads, the same offset time applies to all members when the first member is unreachable. Downloads to the next reachable member do not happen right after a download fails on the unreachable member. The offset time is put in place to prevent all members from performing downloads at the same time.

In the Threat Protection Logging section, define the events per second per rule value to allow the appliance to log events in the syslog:
• **Events per Second per Rule:** Specify the number of events logged per second per rule. The default value is one and the maximum value is 700. Setting the value to 0 (zero) disables the appliance from logging events for the rules. The appliance displays an error message when you enter a value greater than the maximum value. You can override this event filter at the member level.

3. Save the configuration. To publish changes, click **Publish** if it appears at the top of the screen. Note that NIOS does not require restarting of the threat protection service after rule updates.

### Enabling Multiple DNS Requests through a Single TCP Session

The Advance Appliance inspects only one DNS request sent over a single TCP connection. To avoid accepting possible malicious data following a valid DNS request, the appliance terminates the TCP connection after handling the initial DNS request over TCP. You can modify this default Grid setting at the Grid or member level. To modify this setting, do the following:

1. **Grid:** From the **Data Management** tab, select the **Security** tab, and then click **Grid Security Properties** from the Toolbar. **Member:** From the **Data Management** tab, select the **Security** tab -> **Members** tab -> **member** check box, and then click the **Edit** icon. **Profiles:** From the **Data Management** tab, select the **Security** tab -> **Profiles** tab -> **profile** check box, and then click the **Edit** icon.

2. In the **Grid Security Properties** or **Member Security Properties** editor, select the **Threat Protection** tab -> **Advanced** tab, and complete the following:

• **Disable multiple DNS requests via single TCP session:** This is selected by default to avoid accepting possible malicious data following a valid DNS request. When this is selected, the appliance handles the initial DNS request through TCP and then terminates the TCP session to block subsequent DNS traffic, except for an SOA query sent by a client that is accepted in the allow-transfer ACL. This exception covers the case in which an AXFR query follows the SOA query through the same TCP connection. This field is read-only when you use a threat protection profile instead of a ruleset. For more information, see Configuring Grid Security Properties.

3. Save the configuration.

### Configuring NAT Mapping Properties

If you are operating in an environment where you need to aggregate multiple users (such as mobile users) behind one IP address, you might want to consider using NAT (Network Address Translation) Mapping to avoid the potential of service denial to a large group of users if threat protection rules are being applied to the same IP address.

NAT detection is essential to enforce the correct threat protection rule on source IP addresses. The Infoblox NAT Mapping feature allows you to designate individual IP addresses, networks, or ranges along with the source port ranges to denote NAT’ed clients. Any UDP or TCP traffic that originates from an IP address within the NAT IP range and uses a source port within the NAT port mapping is considered as a NAT’ed client. It is important to align the NIOS NAT mapping configuration with the NAT gateway configuration to avoid mis-classification of NAT IPs. Traffic that originates from a given source port block that falls within the configured NAT IP and port range is considered as the same NAT’ed client and traffic that originates from a different port block that falls within the same NAT IP and port range is considered to be a different NAT’ed client. If the traffic originates from the same source IP address, but from a different port block that falls outside the configured port range, then they are considered as a non-NAT’ed client.

NIOS NAT detection is designed to work with a specific form of NAT where multiple clients are NAT’ed onto a single public IP address using a single port block for each client at a time. Some NAT vendors refer to this scheme as PBA (Port Block Allocation) with fixed size port blocks. The NAT device cannot re-use the same NAT IP address for a different client for at least the drop interval of the threat protection rule that is currently running. Note that the client idle timeout duration of the NAT device must be larger than the drop interval of the threat protection rule that is currently running.

You can configure NAT Mapping rules on Advance Appliances by mapping a source IP address, network, or range of IP addresses with a range of ports and specifying the port block size to divide each port range into chunks of port blocks. Each port block represents a single NAT’ed client source port. The IP addresses and the port blocks specified in a NAT Mapping rule may be assigned to the clients in any order, either fixed, sequential, or random.

The appliance logs information about NAT’ed clients to the syslog. Following is an example of the threat detection event log message in the syslog for NAT’ed clients:

```
2015-06-01T22:57:22+00:00 daemon infoblox.localdomain threat-protect-log[12192]: err
CEF:0|Infoblox|NIOS Threat|7.2.0-283371|120303001|Blacklist:block.com|7|src=3.0.0.100
spt=1221 dst=1.1.6.2 dpt=53 act="DROP" cat="BLACKLIST UDP FQDN lookup" nat=1 nfpt=1124
nlpt=1223
```

The following values in the threat detection event log message are specific for NAT’ed clients:

- **nat=1:** Indicates that the syslog event is logged for a NAT’ed client.
- **nfpt:** Indicates the first port in the port block.
- **nlpt:** Indicates the last port in the port block.

For information about the syslog and how to use it, see Viewing the Syslog. Note the following about the NAT Mapping feature:

- A single NAT’ed client cannot use multiple source IP addresses or multiple port blocks simultaneously, otherwise NIOS might consider the same NAT’ed client as different clients.
You can enable the NAT Mapping feature and configure NAT Mapping rules on the Infoblox-4030 Rev-2, Infoblox-4030 10GE appliances and the following hardware-based appliances: PT-1400, PT-1405, PT-2200, PT-2205, PT-2205-10GE, PT-4000, and PT-4000-10GE. Note that you can enable this feature only when threat protection service is enabled on the appliance.

Configuring NAT Mapping Rules

To enable the NAT Mapping feature and to configure NAT Mapping rules for a Grid or a member:

1. **Grid**: From the Data Management tab, select the Security tab, and then click Grid Security Properties from the Toolbar.
   
   **Member**: From the Data Management tab, select the Security tab -> Members tab -> member check box, and then click the Edit icon.

2. In the Grid Security Properties or Member Security Properties editor, select the NAT Mappings tab -> Basic tab, and then complete the following:

   The member inherits the NAT mapping settings from the Grid, by default. To override the settings, click Override. To retain the same settings as the Grid, click Inherit. Note that if you choose to override the Grid settings, you must override the entire setting; you cannot override partial setting.

   - **Enable tracking for NAT mappings**: This check box is disabled by default. When you select this check box, you can configure certain addresses, networks, and ranges for NAT tracking. When the NAT Mapping feature is enabled or disabled for the Grid, all members in the Grid inherit this setting.
   - **NAT Mappings**: To define the NAT Mapping rule, click the Add icon and select one of the following:
     - **Address**: Select this to configure a single NAT address. For example, if you have only one single NAT client or a single NAT source IP, select this.
     - **Network**: Select this if you want to configure an entire subnet for NAT.
     - **Range**: Select this if you want to configure a partial subnet for NAT.

After you select the NAT mapping type, the appliance adds a new row to the table and displays the type in the table (you cannot modify this in the table). In the Address/Network/Range column of the new row, enter a single NAT address, if you have selected Address. You can also configure a network address as a single NAT address. Enter a subnet if you have selected Network; or enter the partial subnet if you have selected Range. Note that IPv6 address, network, or range entry is not supported.

Click + beside the NAT mapping type, and then click the cell of the following fields in the new row to enter information:

- **Start Port**: Enter the first source port in the port range. For example, if the port range is 1000-2000, you can enter 1000 as the start port.
- **End Port**: Enter the end source port in the port range. For example, if the port range is 1000-2000, you can enter 2000 as the end port.
- **Block size**: Enter the port block size. This determines the number of port blocks and each port block is considered as a logical NAT client. Based on the port block size, the port range is divided into port blocks. For example, if the start port is 1000 and the end port is 2000, and if you enter the port block size as 100, then 1000-1099 is the first port block, 1100-1199 is the second port block, 1200-1299 is the third port block, and so on.

You can create a separate NAT Mapping rule for each source IP address, network, or range. You can add a maximum of 32 NAT Mapping rules and a maximum of 32 port ranges for each rule.

**Note**: The combination of the source IP address, network, or range and the port blocks configured for each NAT'ed client must be unique and it should not overlap.

3. Save the configuration.

**Note**: If you change the NAT Mapping rule after you have configured the NAT Mapping rule or if you enable or disable the NAT Mapping feature, you must publish the changes by clicking Publish Changes from the Toolbar. For information, see Publishing Rule Updates.

Managing Threat Protection Rulesets

You can do the following after the initial setup, including uploading the initial ruleset:

- Review the list of threat protection members, as described in Listing Members.
- Look at rulesets that are currently installed on your system, as described in Viewing Threat Protection Rules.
- Upload new rulesets to the system when you have selected to manually apply rule updates, as described in Manually Uploading Rulesets.
• Publish rule updates that you have uploaded to the system, as described in Publishing Rule Updates.
• Modify the Comment and Do Not Delete parameters for an existing ruleset, as described in Modifying Rulesets.
• View differences between an old and a new rulesets and optionally merge rule parameter changes from the old ruleset into the new one, as described in Comparing and Merging Rulesets.
• Configure proxy settings for the Grid if you need to use a proxy server for ruleset updates, as described in Configuring Proxy Servers.
• Delegate ruleset updates to a Grid member and select an alternate interface for downloading the updates, as described in Configuring Members and Interfaces for Automatic Updates.

Listing Members

This panel displays the following information about each Grid member:

• Name: The hostname of the Grid member.
• Status: The status of the DDoS service running on the Grid member.
• Version: Displays the threat protection ruleset version that is currently running on this member. This is displayed in YYYYMMDD-x format, where YYYY is the year, MM the month, DD the date, and x the rule engine version number.
• Comment: Comments that were entered for the Grid member.
• Profile: Displays the threat protection profile that is associated with this member.
• Site: Values that were entered for this pre-defined attribute. You can do the following:
  • Sort the data in ascending or descending order by column.
  • Select a member and click the Edit icon to modify the data.
  • Click the Action icon next to the respective member and:
    • select Permissions from the menu to define permissions for the member.
    • select Clone to new profile from the menu to create a new threat protection profile by cloning the settings from a member to the new profile. Note that this option is enabled only when the selected member is not associated with a profile.
  • Print and export the data in this tab.
  • Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
  • Create a quick filter to save frequently used filter criteria:
    a. In the filter section, click Show Filter and define filter criteria for the quick filter.
    b. Click Save and complete the configuration In the Save Quick Filter dialog box.

The appliance adds the quick filter to the quick filter drop-down list in the panel. Note that global filters are prefixed with [G], local filters with [L], and system filters with [S].

Viewing Threat Protection Rulesets

Grid Manager displays all the rulesets that have been automatically or manually uploaded to the Grid Master. You can drill down to each ruleset to review individual rules in each rule category. To view the current threat protection rulesets and rules:

   Profile: From the Data Management tab, select the Security tab -> Profiles tab -> profiles link.
2. In the Threat Protection Rules or the Members tab or the Profiles tab, Grid Manager displays current rulesets that are stored in the system. It displays the following information for each ruleset:

   • Version: Displays the ruleset version in YYYYMMDD-x format, where YYYY is the year, MM the month, DD the date, and x the rule engine version number. You can click a version link to view rule categories and individual rules in each category for that specific ruleset.
   • Active On: Displays the Grid or the name of the Grid member on which the ruleset is currently running. This can be Grid, a Grid member name, or None. When this displays None, the ruleset is not being used.
   • Do Not Delete: Indicates whether this ruleset can be deleted or not during a ruleset update.
   • Added On: Displays the timestamp when the ruleset was uploaded to the Grid Master in this format: YYYY-MM-DD HH:MM:SS, plus time zone.
   • Add Type: Indicates whether the ruleset was uploaded automatically or manually.
   • Comment: Additional information about this ruleset.

Note: If the member is associated with a profile, the rules become read-only and you cannot edit them when you drill down the ruleset from the Members tab. However, you can still edit the rules if you drill down the ruleset from the Profiles tab even though Grid members are associated with the selected profile.

You can also do the following when you left click the Action icon
Mark a ruleset as do not delete.
Activate, open, or edit a specific ruleset.
Click **Reset to defaults** to globally reset all the rule definitions to their default settings in the selected ruleset. When you reset the ruleset to defaults, all member rulesets will be reset as well. In the **Ruleset Reset** dialog, you can also select **Delete all custom rules in selected ruleset** to remove all the custom rules in the ruleset. You can reset to defaults at the rule category and rule levels. Note that the **Reset to defaults** option is not available if you upgrade to NIOS 7.3.x from a previous release.

To view rules in a specific ruleset version, click the **Version** link and Grid Manager displays the threat protection rules by categories. You can also select the check box of a ruleset and click the **Open** icon to view the rules in the ruleset.

You can also do the following in this panel:

- Manually upload a ruleset by clicking the **Add** icon. For more information, see **Manually Uploading Rulesets**.
- Modify some of the data in the table. Double click a row, and you can modify the **Do Not Delete** and **Comment** columns. Click **Save** to save the changes. Note that other fields are read-only.
- Select the check box of a ruleset and click the **Delete** icon to delete a ruleset, if it is not marked as **Do Not Delete**.

**Note:** When you delete a ruleset that was recently downloaded through automatic downloads, the appliance cannot retrieve or automatically download this ruleset version again. You must manually download the ruleset and then manually deploy it to the Grid. For information about manual downloads, see **Manually Uploading Rulesets**.

- Print or export the data.

Activating a Ruleset

The appliance can store up to nine (9) versions of rulesets. You can switch between these versions and activate one of them as the default ruleset.

To activate a specific ruleset:

1. **Grid:** From the **Data Management** tab, select the **Security** tab -> **Threat Protection Rules** tab.
   
   **Member:** From the **Data Management** tab, select the **Security** tab -> **Members** tab -> **member link.**

2. In the Grid Threat Rulesets or Member Rulesets table, click the **Action** icon and select **Activate** from the menu. In the confirmation dialog, select **Yes** to proceed. The appliance installs the ruleset and uses it as the default ruleset for the Grid or the member.

Overriding the Grid Ruleset

You can override the Grid ruleset for individual members. Note that when a member uses a different ruleset than the Grid, it does not receive a ruleset update if the Grid automatically receives the next update. For information about how to activate a ruleset for the Grid, see **Configuring Grid Security Properties**.

To override the Grid ruleset:

1. From the **Data Management** tab, select the **Security** tab -> **Members** tab -> **member** check box, and then click the **Edit** icon.

2. In the **Member Security Properties** editor, select the **Threat Protection** tab -> **Basic** tab, and complete the following:
   - **Use ruleset:** Click this radio button to edit the ruleset. You can inherit or override a ruleset. When you select to use a ruleset, select an active ruleset from the **Threat Protection Ruleset Version** drop-down list.
   - **Use profile:** Click this radio button to edit the threat protection profile. Click **Select Profile** to select a threat protection profile from the **Threat Protection Profile Selector** dialog box. For more information about threat protection profiles, see **Adding Threat Protection Profiles**.
   - **Active Ruleset Version:** Click **Override** and select a ruleset from the drop-down list. The appliance activates and applies this ruleset to the member. In the confirmation dialog, click **Yes** and the member switches to the selected ruleset. This field is read-only at the member level.
   - **Active Ruleset Comment:** Displays information about the selected ruleset from the **Comment** field. This field is read-only at the member level.

Modifying Rulesets

To modify parameters for an existing ruleset:

1. From the **Data Management** tab, select the **Security** tab -> **Threat Protection Rules** tab.

2. In the Grid Threat Ruleset table, select the ruleset check box, and then click the **Edit** icon.

3. In the **Threat Ruleset** editor, select the **General** tab -> **Basic** tab to modify the following:
• **Comment**: Enter information about the ruleset.
• **Mark as Do Not Delete**: When you select this, the ruleset cannot be deleted during an update. You can select up to three rulesets and mark them as **Do Not Delete**.

You can also view the following information (but you cannot modify it):

• **Version**: Displays the ruleset version in YYYYMMDD-x format, where YYYY is the year, MM the month, DD the date, and x the ruleset engine version number.
• **Active On**: Displays the Grid or the name of the Grid member on which the ruleset is currently running. This can be **Grid**, a Grid member name, or **None**. When this displays **None**, the ruleset is not being used.
• **Added On**: Displays the timestamp when the ruleset was uploaded to the Grid Master in this format: YYYY-MM-DD HH:MM:SS, plus time zone.

### Comparing and Merging Rule Sets

After you manually download a ruleset and before you publish it, you can view differences between the old ruleset and the new one. The appliance shows you the system-level changes, including new rules, deleted rules, and rule syntax, between the two rulesets. It also shows you the customized parameter changes between the two versions. You can then select the changes you want to merge into the new ruleset. You can also modify some of these customized changes before you merge them into the new ruleset. Note that the modifications you make to the customized rule parameters will be added only to the new ruleset. When merging rulesets, all rules in the old ruleset and new ruleset are compared and identified by their rule IDs.

To merge rules from an older ruleset version to a newer ruleset:

1. From the **Data Management** tab, select the **Security** tab -> **Threat Protection Rules** tab, click **Merge** from the Toolbar, and then select **Ruleset** from the drop-down list.
2. In the **Merge Changes Into Ruleset** editor, complete the following:
   • **Old Ruleset**: From the drop-down list, select the ruleset version from which you want to merge changes into the new ruleset. The **Comment** field displays additional information about the ruleset.
   • **New Ruleset**: From the drop-down list, select the ruleset version to which you want the changes to be merged. The **Comment** field displays additional information about the ruleset.
   • **Get Differences**: Click this to display a list of differences between the selected old and new ruleset versions. The appliance displays system-level changes in the **System changes from old ruleset (x items)**, where x is the total number of changed rules between the old and new rulesets. The appliance merges all system-level changes listed in this table into the new ruleset.

The table displays the following information for each changed rule:

• **Rule ID**: The rule ID of the changed rule. You can click the rule link and modify parameters in the rule editor.
• **Rule Name**: The name of the rule.
• **Type**: Indicates whether the rule is a newly added rule or it has been deleted.
• **Old Ruleset Value**: Displays the old value that has been changed.
• **New Ruleset Value**: Displays the newly changed value.

The **Customizations from old ruleset (x items)** table displays customized rule parameter changes between the old and new rulesets, where x is the total number of changed rules. You can select all or specific changed rules in this table to be merged into the new ruleset. You can also modify parameter for selected rules before merging the changes into the new ruleset. This table displays the following information for each rule:

• **Member**: The Grid member on which this rule is currently running.
• **Rule ID**: The rule ID of the changed rule. You can click the rule link and modify parameters in the rule editor.
• **Rule Name**: The name of the rule.
• **Old Ruleset Value**: Displays the old value that has been changed.
• **New Ruleset Value**: Displays the newly changed value.
• **Action**: Displays what the appliance will do to changes in this rule when you merge the rulesets.

3. Click **Merge Changes** to copy all the selected rules and changes you made to specific rules to the new ruleset. Note that you must select a rule from the **Customizations from old ruleset (x items)** table to activate the merging operation.

You can do the following in the **Merge Changes Into Ruleset** editor:

• Click Export to export all the changes listed in both tables to one CSV file. You can export this data after you click **Get Differences** and Grid Manager displays changes in both tables.
• Perform another ruleset merge by selecting another old ruleset and new ruleset.
• Click Close to exit the editor. Note that the editor does not close automatically after a merge.

### Manually Uploading Rulesets

You can download a threat protection ruleset any time when you select to manually perform ruleset updates. You can choose to download rule updates but not immediately deploy them. NIOS archives and tracks up to nine ruleset versions, allowing for switching and merging between these versions when necessary. After uploading a ruleset, you can apply it by publishing it to the Grid and individual members. For more information, see the NIOS Administrator Guide.
information, see Publishing Rule Updates.

Ruleset updates do not require restart of the DNS or threat protection service in the Grid, and they do not affect ongoing services. However, the appliance deploys updated rulesets only when you publish the changes. Note that all threat protection rule update events are logged in the syslog on the Grid Master only.

Note: By default, threat protection ruleset updates are automatic. Infoblox recommends that you retain this setting. For information about how to configure this setting, see Configuring Grid Security Properties.

To manually upload a ruleset file:

1. Access the Infoblox KB article # 2646 by logging in to the Infoblox Support site at https://support.infoblox.com, and then download the ruleset file in the KB article.
2. From the Data Management tab, select the Security tab -> Threat Protection Rules tab, and then click the Add icon.
3. In the Rule File Upload dialog box, do the following:
   - File: Click Select to navigate to the ruleset file location, and then click Upload. Grid Manager displays the file name in this field.
   - Click Test to check the changes that will occur during the rule update, without actually applying the update. You can view the update details in the Syslog Viewer. The appliance preserves the uploaded file if you do not click Update to update the rules. When you manually upload rulesets the next time, this file will be displayed in the dialog. You can then choose to apply the update from this file or upload a new file before performing the update.
   - Click Update to update the rules.
   - Click View Update Results to view the updated rules in the Syslog Viewer. All threat protection rule updates are logged in the syslog on the Grid Master.

Publishing Rule Updates

You can publish rule updates at any time after you have uploaded the ruleset. For information about uploading ruleset files, see Manually Uploading Rulesets.

To publish rule updates:

1. From the Data Management tab, select the Security tab -> Threat Protection Rules tab, and then click Publish Changes from the Toolbar.
2. In the Publish Changes dialog box, complete the following:
   - Publish Changes on all Members: Select one of the following:
     - Simultaneously: Publish changes on all of the members in the Grid at the same time.
     - Sequentially: Publish changes on each Grid member according to the number of seconds you enter in the Sequential every (seconds) field. For example, if you enter every 10 seconds, the system update changes on the first member, and 10 seconds later on the second member. This is the default option.
   - Impacted Members and Services: Click the Poll Members icon to display the affected members in that Grid. Grid Manager displays the member names and whether each member is configured for the threat protection service:
     - Yes: The service is active and the system will publish rule updates on this member upon execution of this task.
     - No: The service is not active and the system will not publish rule updates on this member.
     - Disabled: The service is currently disabled on this member.

To schedule this task, click the Schedule icon at the top of the dialog box. In the Schedule Change panel, complete the following:

   - Now: Publish rule updates upon clicking Publish.
   - Later: Enter the following information to schedule publishing updates at a certain date and time:
     - Start Date: Enter a date in YYYY-MM-DD (year-month-day) format. The appliance displays today’s date. You can also click the calendar icon to select a date from the calendar widget.
     - Start Time: Enter a time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. When you enter the time in a 24-hour format such as 23:00, Grid Manager displays 11:00:00 PM. You can also select a time from the drop-down list by clicking the time icon.
     - Time Zone: Select a time zone for the scheduled date and time from the drop-down list. This field displays the time zone of the browser that the admin uses to log in to Grid Manager.

3. Click Publish to publish changes immediately or click Schedule Publish to schedule the publish.

Delegating Rule Updates to Grid Members

You can delegate ruleset updates to other Grid members if desired. You can also configure the interface you want to use for automatic updates on the members. For information about how to configure this, see Configuring Members and Interfaces for Automatic Updates.

Configuring Threat Protection Profiles

When you configure the Grid or Member security properties, you have an option to select an active ruleset or a threat protection profile. A threat protection profile defines specific security settings and ruleset that you want to apply to a specific member or a group of members. Infoblox uses event filters to limit the amount of logs that are generated due to the threat protection events. It drops packets for services or ports that are not
enabled on the card.
If you want to use the same threat protection rulesets and settings for multiple members, you can create a threat protection profile and associate it with multiple members so you do not have to configure them individually. You can configure threat protection profiles for both hardware and Software ADP appliances. Infoblox automatically migrates threat protection profile settings when:

- you update an active ruleset at the Grid level and if a profile has inherited the respective active ruleset from the Grid.
- the profile inherits an active ruleset from the Grid and you override the active ruleset that is associated with the profile.
- the profile is set to override an active ruleset and you change an active ruleset for the profile.

You can do the following to configure threat protection profiles:

- Create threat protection profiles by associating rulesets, event filters and configuring multiple DNS requests over a single TCP session, as described in **Adding Threat Protection Profiles**.
- Clone threat protection profiles, as described in **Cloning Threat Protection Profiles**.
- Modify threat protection profiles, as described in **Modifying Threat Protection Profiles**.
- View differences between an old and a new rulesets and merge changes from an old threat protection profile into the new one, as described in **Merging Threat Protection Rulesets and Rules**.
- Inherit Grid rule settings for a threat protection profile, as described in **Inheriting Grid Rule Settings**.
- Delete a threat protection profile, as described in **Deleting Threat Protection Profiles**.
- View the list of threat protection profiles, as described in **Viewing Threat Protection Profiles**.

### Adding Threat Protection Profiles

You can create a threat protection profile and associate an active ruleset with it. Infoblox supports common threat protection rulesets for both hardware and Software ADP members. You can either upload a ruleset or download rulesets from a server. You can create any number of threat protection profiles, but you can select only a maximum of five rulesets in combination at the Grid, member and profile levels. For more information about rulesets, see **Understanding Threat Protection Rulesets and Rules**.

The threat protection profile allows you to create your own set of rules for either a member or a group of members that experience a similar kind of traffic. After you define a profile, you can clone it and test the copied settings for a new ruleset on one member before publishing the changes for a group of members that are associated with the profile.

To define threat protection profiles:

1. From the **Data Management** tab, select the **Security** tab -> **Profiles** and then click the **Add** icon.
2. In the **Add Threat Protection Profile Wizard**, add the following:
   - **Name**: Enter a name for the threat protection profile.
   - **Comment**: Enter information about the threat protection profile.
   - **Active Ruleset Version**: Select a value from the drop-down list. This indicates the current ruleset that is used for the respective threat protection profile. If you inherit a ruleset from the Grid and later change the respective ruleset at the Grid level, the new ruleset is not reflected in the profile. You must manually change the selected ruleset for the profile. For more information about active rulesets, see **Understanding Threat Protection Rulesets and Rules**.
   - **Active Ruleset Comment**: Click **Override** to override the comment.
   - **Events per Second per Rule**: Click **Override** to override the values. This indicates the number of events that is logged per second per rule to allow the appliance to log events to the syslog. Specify the number of events logged per second per rule. The default value is one and the maximum value is 700. Setting the value to 0 (zero) disables the appliance from logging events for the rules. The appliance displays an error message when you enter a value greater than the maximum value. You can override this event filter at the member level. For more information, see **Using the Events Per Second Rule Setting**.
   - **Disable multiple DNS requests via single TCP session**: Click **Override** to override the values. This determines if multiple DNS responses through TCP connection are disabled. For more information, see **Enabling Multiple DNS Requests through a Single TCP Session**.

   **Note**: A member associated with a threat protection profile can neither modify **Events per Second per Rule** and **Disable multiple DNS requests via single TCP session** settings at the member level nor enable or disable rules and change rule parameters at the member level.

3. Click **Next** to add extensible attributes.
4. Save the configuration.

### Cloning Threat Protection Profiles

You can create a new threat protection profile by cloning an existing one. The appliance creates a new profile with the settings that are copied from the source profile. You can also associate extensible attributes with the profile. Note that members in the source profile are not carried over to the cloned profile. You must associate new members with the newly cloned profile.

To clone a threat protection profile:

1. From the **Data Management** tab, select the **Security** tab -> **Profiles** and select the threat protection profile that you want to clone, click the **Action** icon.
Threat Extensible Profiles version Rule Protection Profile Selector Members

By default, all ruleset versions, events per second per rule, and disable multiple DNS requests via single TCP session are inherited from items.

(x): All fields are automatically propagated with available information. You can modify the values in the Management Changes: Indicates whether the rule is a newly added rule or it has been deleted.

Rules. (x): All fields are automatically propagated with available information. You can modify the values in the Management Changes: Indicates whether the rule is a newly added rule or it has been deleted.

Profiles. The name of the rule.

Profile Security Profiles Wizard Member Advanc Profile Profiles version Profile Protection Management Changes: Indicates whether the rule is a newly added rule or it has been deleted.

Ruleset Me Security Attributes Ruleset Protection Protection Upd

The table displays the following information for each changed rule:

- **Rule ID:** The rule ID of the changed rule. You can click the rule link and modify parameters in the rule editor.
- **Rule Name:** The name of the rule.
- **Type:** Indicates whether the rule is a newly added rule or it has been deleted.

To merge a threat protection profile:

1. From the Data Management tab, select the Security tab -> Profiles tab, select the threat protection profile that you want to modify, click the Action icon

and then select Edit.

2. The Threat Protection Profile editor contains the following tabs from which you can modify information:
   - **General:** All fields are automatically propagated with available information. You can modify the values in the Basic and Advanced tabs. For more information, see Adding Threat Protection Profiles.
   - **Member Assignment:** Add or delete members that are associated with the respective threat protection profile. Click the Add icon to associate a member with the selected profile. In the Threat Protection Member Selector dialog box, select the member you want to associate with the profile. For more information, see Listing Members. To delete a member that is associated with the profile, select the check box next to the respective member and click the Delete icon.
   - **Extensible Attributes:** Add and delete extensible attributes that are associated with the template. You can also modify the values of the extensible attributes. For more information, see Using Extensible Attributes.

3. Save the configuration.

You must publish the changes after modifying a threat protection profile. For more information about publishing changes, see Publishing Rule Updates.

**Note:** By default, all ruleset versions, events per second per rule, and disable multiple DNS requests via single TCP session are inherited from the Grid unless you click Override to change the Grid settings.

You can merge the threat protection rulesets from one profile to another before you publish it. The following rules are applicable when you update a ruleset that is assigned to a profile and migrate the profile settings to a new ruleset:

- NIOS migrates the profile settings of the rule to the new ruleset when you override a rule, which exists in both the old and the new ruleset, at the profile level.
- The profile ruleset continues to inherit the settings from the Grid if you do not override a rule that exists in both the old and the new ruleset.
- NIOS removes the profile settings for a rule when you override the rule settings for a profile and the rule does not exist in the new ruleset.
- When a rule exists only in a new ruleset, it inherits the settings from the Grid by default.
- Parameters for custom rules are migrated only when the same custom rule exists in the new ruleset.

You can view differences between the old profile and the new one before you publish the changes. The appliance shows you the system-level changes, including new rules, deleted rules, and rule syntax, between the two rulesets and customizations from the old profile. You can then select the changes you want to merge into the new profile. You can also modify some of these customized changes before you merge them into the new profile. When merging profiles, all rules in the old ruleset and new ruleset are compared and identified by their rule IDs. To merge a threat protection profile:

1. From the Data Management tab, select the Security tab -> select either Threat Protection Rules or Members or Profiles tab, click Merge from the Toolbar, and then select Profile from the drop-down list.
2. In the Merge Changes Into Profile Ruleset editor, complete the following:
   - **Old Profile:** From the drop-down list, select the threat protection profile from which you want to merge changes into the new profile. The Comment field displays additional information about the profile and Ruleset version displays the ruleset version.
   - **New Profile:** From the drop-down list, select the threat protection profile to which you want to merge changes. The Comment field displays additional information about the profile and Ruleset version displays the ruleset version.
   - **Get Differences:** Click this to display a list of differences between the old and new profiles. The appliance displays system-level changes in the System changes from old profile (x items) table, where x is the total number of changed rules between the old and new profiles. The appliance merges all system-level changes listed in this table into the new profile.

The table displays the following information for each changed rule:

- **Rule ID:** The rule ID of the changed rule. You can click the rule link and modify parameters in the rule editor.
- **Rule Name:** The name of the rule.
- **Type:** Indicates whether the rule is a newly added rule or it has been deleted.
• **Old Ruleset Value**: Displays the old ruleset value.
• **New Ruleset Value**: Displays the new ruleset value.

The **Customizations from old profile (x items)** table displays customized rule parameter changes between the old and new profile, where x is the total number of changed rules. You can select all or specific changed rules in this table to be merged into the new profile. You can also modify the parameters for selected rules before merging the changes into the new profile. This table displays the following information for each rule:

• **Member/Profile**: The Grid member on which this rule is currently running.
• **Rule ID**: The rule ID of the changed rule. You can click the rule link and modify parameters in the rule editor.
• **Rule Name**: The name of the rule.
• **Old Ruleset Value**: Displays the old ruleset value.
• **New Ruleset Value**: Displays the new ruleset value.
• **Action**: Displays what the appliance will do to changes in this rule when you merge the profiles.

3. Click **Merge Changes** to copy all the selected rules and changes you made to specific rules to the new profile. Note that you must select a rule from the **Customizations from old profile (x items)** table to activate the merging operation.

You can do the following in the **Merge Changes Into Profile Ruleset** editor:

- Click **Export** to export all the changes listed in both tables to one CSV file. You can export this data after you click **Get Differences** and Grid Manager displays changes in both tables.
- Perform another profile merge by selecting another old profile and new profile.
- Click **Close** to exit the editor. Note that the editor does not close automatically after a merge.

**Inheriting Grid Rule Settings**

When you select this option, NIOS automatically inherits the rule settings of the Grid for the respective profile. For example, if you update a rule at the Grid level, you can select this option to reflect the same changes in the profile. To inherit Grid rule settings for the selected profile, from the **Data Management** tab, select the **Security** tab -> **Profiles** tab, select the threat protection profile, click the Action icon

and then select **Inherit Grid Rule Settings**. Click **Yes** in the confirmation dialog box to inherit the settings.

**Deleting Threat Protection Profiles**

When you select this option, NIOS deletes the selected threat protection profile from the database. When you delete a threat protection profile or a profile rule, the appliance puts them in the Recycle Bin, if enabled. You can restore them if necessary. Note the following about threat protection profiles:

- When you delete a profile that contains an active ruleset, which is overridden at the profile level, you can restore the profile including the configuration if the ruleset exists on the Grid. You cannot restore the profile if the ruleset is deleted.
- When you delete a profile that inherits ruleset from the Grid, and if the same ruleset is still active on the Grid, you can restore the profile including the configuration for profile rules. If the ruleset is deleted or if the active ruleset on the Grid has changed, the appliance restores the profile from the Grid along with the profile rule settings for the current active ruleset.

To delete a threat protection profile, from the **Data Management** tab, select the **Security** tab -> **Profiles** tab, select the threat protection profile that you want to delete, click the Action icon

and then select **Delete**. Click **Yes** in the confirmation dialog box to delete.

**Viewing Threat Protection Profiles**

To view the list of threat protection profiles:

1. From the **Data Management** tab, select the **Security** tab, and then click the **Profiles** tab. Grid Manager displays the following information:
   • **Name**: The name of the threat protection profile. Click the **profile** name to view the rules that are associated with the selected threat protection profile. For more information about rules, see **Viewing Threat Protection Rules**.
   • **Version**: The version of the threat protection profile.
   • **Members**: Displays the member associated with the threat protection profile. You can sort the values in this column.
   • **Comment**: Displays information that you specified for the threat protection profile.
   • **Site**: The location to which the member belongs. This is one of the predefined extensible attributes.

You can also do the following:

- Use **Global Search** to search for threat protection profiles by name, comment or object type. For information, see **Using Global Search**.
- Use **Smart Folders** to organize threat protection profiles by name, comment or object type. For information, see **About Smart Folders**.
- To export the entire list of threat protection profiles in a csv format, click the Export icon and choose **Export Data in Infoblox CSV Import Format**. It also exports the customized rules for the profile. For more information, see **Exporting Data to Files**. To export all data in a
Managing Threat Protection Rules

You can modify any previously defined custom rules, or some of the parameters for system and auto rules. For most system and auto rules, you may change the Action and Log Severity. You can also enable or disable individual rules or an entire category of rules.

If you have selected to manually update threat protection rules, you must download updated rules from the Infoblox Support web site and then publish them to the system.

When a member is associated with a profile, it automatically uses the ruleset that is associated with the profile. When you delete the associated profile, member uses the ruleset that was previously associated with it.

You can do the following after the initial setup, including uploading the initial ruleset:

- Look at rules that are currently installed on your system, as described in Viewing Threat Protection Rules.
- Enable and disable certain rules, as described in Enabling and Disabling Rules.
- Upload rule updates to the system when you have selected to manually apply rule updates, as described in Modifying System and Auto Rules.
- Publish rule updates that you have uploaded to the system, as described in Publishing Rule Updates.
- Modify existing system rules, as described in Modifying System and Auto Rules.
- Modify custom rules, as described in Modifying Custom Rules.

Viewing Threat Protection Rules

You can view the threat protection rules in one of the following views:

- Click Toggle Flat View to display a flat list of all the threat protection rules. In the flat view, each of the custom, system, and auto rules are listed separately.
- Click Toggle Tree View to display only the category of threat protection rules. You can expand the category of rule to view individual rules listed in each category.

To view rules categories and individual rules in a specific ruleset version:

1. **Grid**: From the Data Management tab, select the Security tab -> Threat Protection Rules tab. **Member**: From the Data Management tab, select the Security tab -> Members tab -> member link. **Profile**: From the Data Management tab, select the Security tab -> Profile tab -> profile link.
   
2. In the Grid Security or Member Security table, click the Version link and Grid Manager displays the threat protection rules by categories. The Category column lists all the category to which rules belong.

3. To view individual rules listed in each category, expand the list by clicking the arrow beside the check box. You can view the following information for each rule:
   
   - **Category**: The category to which the rule belongs.
   - **Order**: The number that indicates the order in which the rule will be executed by the appliance. The rule order can change during a ruleset update.
   - **Rule ID**: The ID of the rule.
   - **Rule Name**: The name of the rule. This can contain up to 255 characters.
   - **Type**: The rule type. This can be Custom, System, or Auto. For more information about each rule type, see Understanding Threat Protection Rulesets and Rules.
   - **Disabled**: Displays whether the rule is disabled. A disabled rule does not perform any mitigation functions.
   - **Comment**: Comments that were entered for the rule. This can contain up to 255 characters.
   - **Action**: The operation that the appliance performs when the event occurs. This can be one of the following:
     - **Alert**: The appliance passes the packets and logs the event.
     - **Drop**: The appliance drops the packets and logs the event.
     - **Pass**: The appliance passes the packets but does not log the event.
- **Description**: Description about the rule. This can contain up to 255 characters.
- **Rule Parameters**: Displays the rule parameters that are configured for the rules and the corresponding values for the rule parameters.
- **Log Severity**: Log severity level. This can be **Critical**, **Major**, **Warning**, or **Informational**.

You can also do the following in this panel:

- Click the Action icon

  and select one of the following actions for a rule category:

  - **Enable All Rules in Category**: Select this to enable all the rules in the selected category. For a Grid member, this action overrides the Grid rule settings.
  - **Disable All Rules in Category**: Select this to disable all rules in the selected category. For a Grid member, this action overrides the Grid rule settings.
  - **Inherit Grid Rule Settings in Category**: Select this to inherit Grid rule settings for the selected category. This appears only for member settings.

- Modify some of the data in the rules table. Double click a row, and modify the data. Click **Save** to save the changes. Note that some fields are read-only.

- Select the check box of a rule and click the **Edit** icon to modify the properties of the rule.

- Select the check box of a custom rule and click the **Delete** icon to delete a custom rule.

- Print or export the data.

- Publish changes you make to the rules by clicking **Publish Changes** from the Toolbar. For more information, see **Publishing Rule Updates**.

- Use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.

**Note**: When you use the **Go to** function to search for specific rules, Grid Manager may return duplicates of the same rules due to the paging mechanism currently used for displaying information.

- Create a quick filter to save frequently used filter criteria. For more information, see **Using Quick Filters**.

### Using Quick Filters

You can use the following quick filters to filter threat protection rules in the Grid Rules panel. When you select a filter, Grid Manager displays only the specified rules. Using filters makes it easier to locate specific rules for editing, enabling, and disabling.

- **All Auto Generated Rules**: This option shows all auto-generated rules defined in the Infoblox Advanced DNS Protection solution.
- **All Custom Rules**: This option shows all whitelisting and blacklisting custom rules defined by NIOS users.
- **All System Rules**: All protocol-specific rules associated with particular attack phenomena.
- **All Disabled Rules**: This option shows all disabled rules.
- **All Enabled Rules**: This option shows all enabled rules.

For more information about filters, see **Using Filters**.

### Enabling and Disabling Rules

By default, all activated threat protection rules apply across the entire Grid. Enabling or disabling a rule category will enable or disable all rules contained in that category. You can also enable or disable individual rules.

**To enable or disable all rules in a category, do the following:**

1. Grid: From the **Data Management** tab, select the **Security** tab → **Threat Protection Rules** tab, and then click the ruleset link.
   
   Member: From the **Data Management** tab, select the **Security** tab → **Members** tab, and then select a member and click the ruleset link.

2. In the Threat Ruleset table, click the Action icon

   next to the rule category, and choose **Enable All Rules in Category** or **Disable All Rules in Category**. Either option can be disabled depending on the current state of the rules in the category. For members, you can select **Inherit Grid Rule Settings in Category** to inherit rule settings from the Grid.

**To enable or disable individual rules, do the following:**

1. Grid: From the **Data Management** tab, select the **Security** tab → **Threat Protection Rules** tab, and then click the ruleset link.
   
   Member: From the **Data Management** tab, select the **Security** tab → **Members** tab, and then select a member and click the ruleset link.

2. Click the arrow beside a rule category to expand all rules in a rule category.

3. Click the Action icon

   next to a rule and choose **Enable** or **Disable** from the menu. Either option can be disabled depending on the current state of the rule.
Note: Depending on the nature of the rules, you may or may not be able to disable or enable certain rules.

Modifying System and Auto Rules

1. From the Data Management tab, select the Security tab -> Threat Protection Rules tab.
2. In the Grid Rules table, expand the category to which the rule belongs, select the check box, and then click the Edit icon.
3. In the System Rule or Auto Generated Rule editor, select the Description tab -> Basic tab to modify the following:
   - Comment: Enter information about the system rule.
   - Disable: Select this check box to disable the system rule. You cannot disable auto rules. You can also view the following information (but you cannot modify it):
     - Rule ID: Displays the rule ID of the system rule.
     - Name: Displays the name of the rule.
     - Category: Displays the category to which the system rule belongs.
     - Description: Displays the description of the system rule.
   - Order: Displays the number that indicates the order in which the rule will be executed by the appliance. The rule order can change during a ruleset update.
4. In the System Rule or Auto Generated Rule editor, select the Settings tab -> Basic tab. Depending on the rule, you may or may not be able to modify the following:
   - Action: Displays one of the following: Alert, Drop or Pass. Some rules are restricted to specific actions. For example, the action for all blacklisting rules is set as Drop, where the appliance drops the packets and logs the activity when such an event occurs. The action for all whitelisting rules is set as Pass, where the appliance silently passes the packets without logging when such an event occurs.
     - Alert: Logs the activity, and passes the packet.
     - Drop: Logs the activity and drops the packet.
     - Pass: Silently passes the packet without logging.
   - Log Severity: Select the log severity level from the drop-down list. You can select Critical, Major, Warning, or Informational. The selection here corresponds to the severity levels you configure for logging in the syslog.
   - Rule Parameters: In the Rule Parameters table, the Description column displays the rule parameters. Click the row and enter the corresponding values for the rule parameters in the Value column. Depending on the rule, this table displays only the parameters that are relevant to the system or auto rule.
5. Save the configuration.

Modifying Custom Rules

1. From the Data Management tab, select the Security tab -> Threat Protection Rules tab.
2. In the Grid Rules table, expand the category to which the rule belongs, select the check box, and then click the Edit icon.
3. In the Custom Rule editor, select the General tab -> Basic tab to modify the following:
   - Comment: Enter information about the custom rule.
   - Disable: Select this check box to disable the custom rule.
   You can also view the following information (but you cannot modify it):
     - Template: Displays the name of the template the custom rule uses.
     - Rule ID: Displays the rule ID of the custom rule.
     - Name: Displays the name of the rule.
     - Category: Displays the category to which the custom rule belongs.
     - Description: Displays the description of the custom rule.
4. In the Custom Rule editor, select the Settings tab -> Basic tab to modify the following:
   - Log Severity: Select the log severity level from the drop-down list. You can select Critical, Major, Warning, or Informational. Log severity may have an effect on how other Grid services respond to particular events. The selection here corresponds to the severity levels you can configure for logging in the syslog.
   - Rule Parameters: In the Rule Parameters table, the Description column displays the rule parameters. Click the row and enter the corresponding values for the rule parameters in the Value column.
   - Action: Displays the operation which the appliance performs when this event occurs. Some rules are restricted to specific actions. For example, the action for all blacklisting rules is set as Drop where the appliance drops the packets and logs the activity when such an event occurs. The action for all whitelisting rules is set as Pass, where the appliance silently passes the packets without logging when such an event occurs.
5. Save the configuration.

Monitoring Threat Protection Events

You can monitor threat protection events through the following:
- Syslog, as described in Monitoring through Syslog.
Monitoring through Syslog

To receive threat protection events in the syslog, you must enable the Security option in the DNS logging category of the Grid DNS Properties editor. For information about configuring the logging category, see Setting DNS Logging Categories. Once the Security option is enabled, hardware-based appliances log each threat protection related event in the syslog in CEF (Common Event Format). You can get detailed information about the events by reviewing the syslog periodically. For information about how to configure the syslog server, see Using a Syslog Server.

When a DNS attack is detected against an enabled rule, the appliance generates a log message. Note that only threat protection messages in CEF are displayed in the syslog. The log messages for rate limiting alert events also include the FQDNs extracted from DNS queries whose standard query and question count is greater than zero so you can quickly identify the offending clients. Note that the FQDN field displays “NA” for invalid DNS queries. This feature is enabled by default. You can disable this only in Maintenance Mode using the CLI command set smartnic-debug-adp-log-fqdn off.

Example:

When the appliance detects ICMP ping attacks that exceed the pint size against an existing auto rule that has the following configuration:

- Log Severity = Critical
- Rule ID = 120600925
- Rule Name = Potential DDoS related domain
- Rule Action = Drop
- Rule Category = Potential DDoS related Domains

It generates the following threat detection event log message:

```
2016-03-30T12:30:17-07:00 daemon ol-18-114.tme.infoblox.com
threat-protect-log[15396]: err adp: CEF:0|Infoblox|NIOS
Threat|7.3.2-316478|120600925|Potential DDoS related domain:
uuu9.com|7|src=10.10.50.62 spt=60154 dst=25.11.11.114 dpt=53 act="DROP"
cat="Potential DDoS related Domains" nat=0 nfpt=0 nlpt=0 fqdn=lol.uuu9.com
```

The number of log messages generated is based upon your Event per Second per Rule setting. For example, if the setting is 5, the appliance generates five log messages of the same event per second when the attack continues within the time duration. Each log message contains the following information:

- The timestamp when the event happened in yyyy-mm-ddThh:mm:ss+00:00 format.
- **Infoblox|NIOS Threat|x.x.x**: Indicates the Infoblox product, and x.x.x represents the NIOS version.
- The number following the NIOS version is the rule ID. In this example, it is 120600925.
- Following the rule ID is the rule name specified in the rule.
- Following the rule name is the log severity. The following numbers indicate the severity levels:
  - 8 = Critical
  - 7 = Major
  - 6 = Warning
  - 4 = Informational
- **src**: Source IP address.
- **spt**: Source port.
- **dst**: Destination IP address.
- **dpt**: Destination port.
- **act**: The rule action, which can be ALERT, DROP, or PASS, depending on the rule configuration.
- **cat**: The rule category to which the rule belongs. In this example, the rule category is “Potential DDoS related Domains.” For information about rule categories, see System and Auto Rule Categories.

To view DNS threat protection related log messages:

1. From the Administration tab, select the Logs tab -> Syslog tab.
2. From the drop-down list at the upper right corner, select the Grid member on which you want to view the syslog.
3. From the Quick Filter drop-down list, select Threat Rule Update Events or Threat Detection Event Logs to view rule update events or threat detection events respectively. To narrow down the system messages you want to view, click Show Filter and then select the filters you want to use. For information about how to use filters, see Using Filters.

Threat Protection Statistics Widget

You can also get a high-level view of the threat protection events through the Status Dashboard. The Advance Appliances provide the Threat Protection Statistics widget so you can monitor the trend and counts of the various events. For more information about the Dashboard and the Threat Protection Statistics widget, see Status Dashboards.

Threat Protection Reports
NIOS provides a series of reports to monitor and analyze DNS threat protection events. When you integrate a reporting member in your Grid, you can get the threat protection both hardware and Software ADP related reports so you can monitor event counts by severity, member, rule, and rule category. Note that all reporting traffic goes over the MGMT port on the reporting member by default. If for any reasons you need to configure a different interface for the reporting traffic, you can do so through the reporting Member Properties editor. For detailed information about these reports and how to configure the interface for reporting traffic, see Security.

DNS and Network-Flood Threats

DNS is a tempting target for attacks given that it is a core Internet service. Attackers can send malformed DNS queries or DNS responses to the targeted server, hoping to exploit bugs in its DNS implementation. Other variants include code insertion, buffer overflows, memory corruption, NULL pointer dereferencing, and specific vulnerability exploits.

DNS attacks tend to follow specific patterns but can be difficult to deal with using only rate-limiting techniques, because of the sheer scale of many recent attacks. DNS threat protection is designed to grow and expand over time, through threat protection rule updates, to deal with both outside-in and inside-out attacks on network infrastructure and Internet services.

Following are some of the network-flood attacks that can target your DNS caching and authoritative servers:

Internet Control Message Protocol (ICMP) Flood

An ICMP flood attack is also known as a ping attack in which attackers send a large number of ICMP ping packets to a DNS server repeatedly in order to hinder the server’s ability to respond to other requests. It can also be an attempt to send a large number of ping packets to the broadcast IP of a subnetwork, otherwise known as a Smurf attack, as a basic means of amplifying an attack across more hosts than a normal ping would typically permit. These types of attacks can be dealt with by setting a policy to disallow pings to the broadcast IP on the network.

Note: When threat protection is enabled, ICMP ping size (for IPv4 and IPv6) is limited to 16,000 bytes.

SYN Flood

A host sends a long stream of TCP SYN packets, frequently using a forged sender address. Because TCP regards a SYN packet as part of a legitimate connection request, the requested server starts a half-open connection by responding with a SYN ACK packet. Since the sender address is faked, the final ACK response from the sender never comes, and the half-open TCP socket closes only after a time out interval. A massive wave of SYN requests with fake senders can wipe out the connection resources of a network device, effectively locking it away from legitimate users.

UDP DNS Flood

UDP Flood is a denial-of-service attack that uses the connectionless UDP transport protocol and attempts to send large numbers of packets to random UDP protocol ports on a remote system, or to a specific protocol. UDP flood is a reflection attack that is often used for attacking DNS servers operating on UDP port 53. UDP flooding typically uses IP spoofing, in which the sender address is faked. The purpose is to occupy so many resources on the target that it can no longer provide its services on the network.

Inside-Out Attacks

A sophisticated form of "phishing" in which an attacker is able to inject a worm or other piece of attack software onto a host machine, which thereupon captures sensitive information such as logins, and adds that data to DNS queries that can be sent from the trusted machine to an untrusted entity for collection. DDoS Security detects data leaks of this type, logs the incident, and funnels the suspect packets to a quarantine location. In a similar vein, DNS Tunneling uses DNS as a covert channel to avoid firewall and IPS security mechanisms. Tunneling encapsulates Inbound and outbound packets inside DNS requests and DNS responses.

DNS Fluxing

the use of a system called a Domain Generation Algorithm botnet to perform one of the following attacks:

- **Fast Fluxing**: Forcing rapid swapping in and out of IP addresses, with extremely high frequency through changing DNS records with brief TTLs
- **Domain Fluxing**: Forcing constant changing of and allocation of multiple fully-qualified domain names (FQDNs) to a single IP address on the recursive or authoritative DNS server.

DNS Cache Poisoning

With cache poisoning, attackers attempt to insert a spoofed DNS response to a DNS resolver, which then stores the response in its cache, where it lives until the TTL expires. The cache is poisoned and subsequent requests for the domain address to recursive name servers are answered with the address of a different server, presumably controlled by the attacker. So long as the fake entry resides in the DNS server cache (persistence of a cache entry is usually governed by time to live) it can result in hundreds of thousands of dangerous redirects. In such cases the URL is legitimate, but the destination servers are not. This process is often called a "pharming" attack. Web servers and mail servers are frequent targets. Other redirection attacks include DNS Changer and DNS Replay. Man-in-the-middle is another descriptive term for many redirection attacks.
DNS Reflection and Amplification Attacks

As with UDP flood, DNS reflection attacks use a form of IP spoofing, changing the source address in their DNS queries to show the address of their intended target, such as a DNS root server or a top-level domain (TLD) name server operator. DNS reflection and amplification recognizes UDP as an asymmetrical protocol (small requests, large responses) and the existence of open DNS resolvers to the Internet cloud. The result is that small DNS queries reflect large UDP datagram responses to the target address in the original source datagrams. Some recent attacks have used this DDoS technique at a huge scale. Because DNS runs over UDP and does not require a handshake, it is possible to use the protocol as a means to lock down a host or a network. Designed a specific way, sending a small query to any open DNS resolver can result in a single response containing several kilobytes or more, that are sent to the unwitting spoofed victim. (This type of response typically is sent via TCP, as UDP does not allow for more than 512 bytes in a response datagram. The resulting packet usually exceeds the MTU of the recipient’s interfaces, resulting in further packet fragmentation and processing.) Open DNS resolvers may allow for launching DDoS attacks containing hundreds of gigabytes of data. Attackers may also use the EDNS0 DNS protocol extension as a means to enable larger DNS responses. Many network operators, particularly overseas, allow open DNS resolvers to run on their networks, unwittingly allowing attackers to abuse them. Many network operators do provide intelligent rate-limiting to prevent abuse, even while supporting open recursive DNS servers. Hence, issues of this type usually result from mistakes in configuration.

DNS Malware

Sophisticated malware also has emerged as a serious threat to DNS infrastructure. They are classified as Advanced Persistent Threats, and use DNS to embed themselves in the target network and stealthily communicate with external command servers to obtain malware updates, instructions, and to conduct attacks for data theft, industrial espionage and other goals.

DNS Domain Hijacking

Domain hijacking or domain theft is the act of changing the registration of a domain name without the permission of its original registrant. Domain hijacking is generally done by exploiting a vulnerability in the domain name registration system or through social engineering. In some cases however, domain hijackers alter the DNS data of a domain after gaining control of it. They consequently redirect users to a fraudulent site, instead of the legitimate site, on the Internet.

To protect your authoritative DNS server against DNS domain hijacking, you can configure the appliance to monitor NS records and glue records of top-level authoritative zones. Based on your configuration, the appliance periodically checks DNS data in the NS RRsets for these zones and compares the data with that in the appliance database. It then reports any data discrepancies through SNMP traps and logs related events in the syslog. You can also monitor the status of DNS data discrepancies, if any, through the DNS Integrity Check widget on the Task Dashboard. The severity in data discrepancies can help identify possible domain hijacking. For more information about how to configure this feature, see About DNS Integrity Check for Authoritative Zones.

Chapter 43 Infoblox DNS Firewall

This chapter provides information about the Infoblox DNS Firewall feature that you can configure and manage on the Infoblox appliance. It includes the following sections: About Infoblox DNS Firewall

- About Infoblox DNS Firewall
- Setting Up Infoblox DNS Firewall
- License Requirements and Admin Permissions
  - For Local RPZs and RPZ Feeds
  - Grid-wide licenses for RPZ
  - For FireEye Integrated RPZs
- Best Practices for Configuring RPZs
  - General RPZ Best Practices
  - Best Practices For FireEye Integrated RPZs
- Enabling Recursion for RPZs
  - Configuring RPZs for All Recursive Servers
  - Enabling and Disabling RPZ Query Name Recursion
- Configuring Local RPZs
- Configuring Rules for RPZs
  - Managing Passthru Rules
  - Managing Block (No Such Domain) Rules
  - Managing Block (No Data) Rules
  - Managing Substitute (Domain Name) Rules
  - Managing Substitute (Record) Rules
- Configuring Infoblox Threat Intelligence Feed
  - Infoblox Threat Intelligence Feeds
- Downloading Rules for an RPZ Feed
- Testing RPZ Feed Rules
- About FireEye Integrated RPZs
  - Configuring FireEye RPZs
  - Configuring Rules for FireEye RPZs
  - Configuring the FireEye appliance
  - Handling Alerts from the FireEye appliance
  - Logging FireEye Integrated RPZ messages
  - Configuration Examples
Mitigating Cyber Threats using TAXII
- Licensing Requirements and Permissions
- Mapping RPZs with TAXII Collections
- Extensible Attributes for TAXII Service
- Monitoring TAXII Server

Managing RPZs
- Viewing RPZs
- Modifying RPZs
- Reordering RPZs
- Locking and Unlocking RPZs

Managing RPZ Rules
- Viewing RPZ Rules
- Modifying RPZ Rules
- Deleting RPZ Rules
- Copying RPZ Rules
- Importing RPZ Rules
- Disabling NSDNAME and NSIP rules for RPZ zones

Licensing Requirements and Permissions
- Mapping RPZs with TAXII Collections
- Extensible Attributes for TAXII Service
- Monitoring TAXII Server

Monitoring TAXII Server

Managing RPZs
- Viewing RPZs
- Modifying RPZs
- Reordering RPZs
- Locking and Unlocking RPZs

Managing RPZ Rules
- Viewing RPZ Rules
- Modifying RPZ Rules
- Deleting RPZ Rules
- Copying RPZ Rules
- Importing RPZ Rules
- Disabling NSDNAME and NSIP rules for RPZ zones

Extensible Attributes for TAXII Service
- Mapping RPZs with TAXII Collections
- Extensible Attributes for TAXII Service
- Monitoring TAXII Server

Monitoring TAXII Server

About Infoblox DNS Firewall

Infoblox DNS Firewall employs DNS RPZs (Response Policy Zones), a technology developed by ISC (Internet System Consortium) for allowing reputable sources to dynamically communicate domain name reputation so you can implement policy controls for DNS lookups.

On an Infoblox appliance, you can configure RPZs and define RPZ rules to block DNS resolution for malicious or unauthorized hostnames, or redirect clients to a walled garden by substituting responses. You can assign actions to RPZ rules. For example, abc.com can have an action of pass thru or substitute (domain) with the domain xyz.com. You can also configure a Grid member to act as a lead secondary that receives RPZ updates from external reputation sources and redistributes the updates to other Grid members. Infoblox DNS Firewall supports both IPv4 and IPv6 networks. It also facilitates the detection of malware and APTs (Advanced Persistent Threats) by integrating the NIOS appliance with a FireEye appliance. You can employ APT mitigation strategy using FireEye as an external threat detection source.

An Infoblox Grid performs RPZ actions for queries that originate from external sources. The name server recursive cache on an RPZ enabled Grid member uses the address of the client from which the query originates to identify if the query is generated from an external source or an internal Grid. If the query originates from a Grid Master or a Grid member that has RPZ license installed, RPZ actions are automatically bypassed for those queries. For RPZ, Infoblox uses the ACL infoblox-deny-rpz, which contains a list of addresses for bypassing RPZ actions. The infoblox-deny-rpz list excludes Grid members that do not have an RPZ license. Note that RPZ action is performed only once for a single recursion.

As illustrated in Figure 42.1, the Infoblox DNS server receives RPZ updates, which include blacklisted hostnames and responses, from a reputation data server through a DNS zone transfer. The appliance then blocks or redirects queries and responses based on the imported RPZ rules. The reporting server can then generate the DNS Top RPZ Hits report that details the top DNS clients that have received redirected responses through RPZs.

Figure 42.1 Infoblox DNS Firewall
There are three types of RPZs:

- **Local RPZ** – A local RPZ is a zone that allows administrators to define multiple response policies locally. Responses sent are based on the defined rules. For information about how to configure local RPZs, see [Configuring Local RPZs](#).
- **RPZ Feed** – An RPZ feed receives response policies from external sources. DNS clients receive responses based on the imported rules from a reputable source, such as a commercial RPZ provider. For information about RPZ feed, see [Configuring Infoblox Threat Intelligence Feed](#).
- **FireEye integrated RPZ** – By integrating the NIOS appliance with the FireEye appliance, you can detect malware and APTs and take necessary actions to mitigate those threats. For information about FireEye integrated RPZ, see [About FireEye Integrated RPZs](#).

**Note:** You can configure up to a total of 32 RPZs, including local and FireEye integrated RPZs.

### Setting Up Infoblox DNS Firewall

For a successful Infoblox DNS Firewall deployment to protect your endpoint devices and servers from stealthy malware and malicious hostnames, consider the guidelines described in [Best Practices for Configuring RPZs](#). To configure Infoblox DNS Firewall, complete the following tasks:

1. Install a valid RPZ license on the appliance, as described in [License Requirements and Admin Permissions](#). For more information about RPZ licenses, see [License Requirements and Admin Permissions](#).

**Note:** Ensure that you have installed a valid DNS license on the same appliance.

2. Enable recursive queries for a DNS view, member, or Grid, as described in [Enabling Recursion for RPZs](#).

**Note:** Ensure that you enable recursive queries for RPZ rules to take effect.

3. Configure RPZ logging to ensure that all matching and disabled rules for all queries are logged in the syslog. You can view the syslog to ensure that the rules are set up correctly before they take effect. Ensure that you enable `rpz` in the **Logging Category** of Grid DNS Properties editor to log these events. For information about how to set logging categories, see [Setting DNS Logging Categories](#).

4. You can configure a local RPZ, an RPZ feed, or a FireEye RPZ on the NIOS appliance. Complete one of the following depending on your selection:

   - **On a DNS member, complete the following to create local RPZ rules:**
     - a. Create an RPZ, as described in [Configuring Local RPZs](#).
     - b. Configure rules for the local RPZ you have created, as described in [Configuring Rules for RPZs](#).

   - **Optionally, complete the following to receive RPZ updates from an RPZ feed:**
     - a. Configure an RPZ feed, as described in [Configuring Local RPZs](#). You can also configure the Infoblox DNS feed, as described in [Configuring Infoblox Threat Intelligence Feed](#). The Infoblox DNS feed is a reputable data server validated by Infoblox to provide reputation RPZ updates.
b. Download rules from the RPZ feed, as described in Downloading Rules for an RPZ Feed.

- Optionally, complete the following to receive alerts from a FireEye appliance:
  a. Create a FireEye integrated RPZ, as described in Configuring FireEye RPZs.
  b. Define rules for FireEye RPZs, as described in Configuring Rules for FireEye RPZs.
  c. Create FireEye admin users, as described in Configuring the FireEye appliance.
  d. Add URLs and user credentials on the FireEye appliance, as described in Configuring FireEye RPZs.

Note: To apply the configured RPZ policies regardless of whether a DNS query requests DNSSEC data, configure the appliance accordingly. For more information about how to configure this, see Applying Policies and Rules to DNS Queries that Request DNSSEC Data.

5. Test your RPZ configuration and verify that RPZ is functioning properly by viewing the syslog and the Last Updated column in the Response Policy Zones tab. For more information, see Testing RPZ Feed Rules.

After you have set up your RPZs, RPZ feeds, and RPZ rules, you can do the following:

- Manage local RPZs such as viewing a list of RPZs, modifying, reordering, and deleting RPZs. You can also lock or unlock RPZs. For more information, see Managing RPZs.
- Verify RPZs are functioning properly by viewing the syslog and the last updated RPZ. For more information, see Managing RPZ Rules.
- Manage Local RPZ rules such as viewing, modifying, and deleting RPZ rules. You can also copy and import RPZ rules. For more information, see Managing RPZ Rules.
- Generate the DNS Top RPZ Hits report, if you have a reporting server set up in the Grid. For more information, see DNS Top RPZ Hits.
- Define thresholds for RPZ hit rate and configure the appliance send alerts when the RPZ hit rate exceeds the thresholds. For information, see Configuring Thresholds for RPZ Hit Rate.

License Requirements and Admin Permissions for RPZ

You must install required licenses before you can use the RPZ feature. An RPZ license is required to configure local RPZs and RPZ feeds. For more information, see For Local RPZs and RPZ Feeds. For FireEye integrated RPZs, you must first install an RPZ license, and then a FireEye license. For more information, see For FireEye Integrated RPZs. For all RPZ related licenses, you can install either a temporary or a permanent license on the NIOS appliance. The temporary license provides a 90-day free trial, which can be upgraded to a permanent license. After the license expires, the RPZs will remain intact, but you cannot delete existing or add new entries to it. Infoblox provides RPZ licenses that are compatible with each product model.

For Local RPZs and RPZ Feeds

Before you install an RPZ license, ensure that the following are completed:

- The entire Grid is running NIOS 6.6 or later.
- Grid members are properly configured and DNS is enabled on the members.

Note: Install RPZ licenses only on Infoblox members that have DNS recursion enabled.

Superusers can configure RPZs and RPZ rules by default. You can also assign global permissions for all RPZs and RPZ rules to specific admin groups and roles. For more information, see Administrative Permissions for Zones.

Grid-wide licenses for RPZ

Infoblox offers a Grid-wide ActiveTrust Plus and ActiveTrust Advanced additional services for DNS Firewall feature. These are subscription licenses that you may have to purchase from Infoblox. When you purchase these services, you can use the ActiveTrust threat subscription data on any appliance that can run DNS Firewall across the Infoblox Grid which you have configured. You can buy these additional services if you do want to use Infoblox threat data and instead use your own or an external threat feed. With these additional services, you get to use a separate license key for each Grid that you use.

When you configure Grid-wide RPZ license for each Grid, RPZ rules are not applied for queries that originate from the other RPZ member(s) of the Grid. When you use multiple Infoblox Grids, you can use the same TSIG key to configure feed zones across all Grids to synchronize feed subscriptions. Note that these services are valid for NIOS versions 8.0 and above. For more information, see Managing Grid-wide Licenses. For a thorough understanding of the RPZ process using various NIOS versions, consider a scenario where you have configured four members on the Grid: GM(RPZ license), M1(RPZ license), M2(DNS license), M3(RPZ license), and RM1 (Reporting Member).

- In NIOS version 7.3, all members with RPZ licenses are added to the ACL list:
  ```
  infoblox-deny-rpz { localhost; GM_IP, Member1_IP; Member3_IP; }
  ```
- In NIOS version 8.x:
  ```
  infoblox-deny-rpz { localhost; GM_IP, Member1_IP; Member3_IP; }
  ```

  - When you install a Grid Wide RPZ license, all members with DNS licenses are added to the ACL list:
infoblox-deny-rpz { localhost; GM_IP, Member1_IP; Member2_IP; Member3_IP; }

- When you install a Grid Wide RPZ license, but not a member level RPZ license, NIOS adds all the members with DNS licenses to the ACL list:

infoblox-deny-rpz { localhost; GM_IP, Member1_IP; Member2_IP; Member3_IP; }

- When you do not install a Grid-wide RPZ license but install member-level RPZ licenses, NIOS adds all members that have RPZ licenses to the ACL list and enables the **Apply RPZ rules only on this member if possible** check box for that member. You can clear the check box.

infoblox-deny-rpz { localhost; GM_IP, Member1_IP; Member2_IP; Member3_IP; }

**Note:** Infoblox suggests that when you upgrade to NIOS 8.0 and later versions, select the check box **Apply RPZ rules only on this member if possible** only if there is an existing RPZ license for the Grid member to ensure that there is no change in behavior due to an upgrade.

Note the following about Grid-wide licenses for RPZ:

- NIOS displays `rpz` in the Grid-wide and Member tabs when RPZ license is installed.
- When you enable a temporary license for RPZ, it is enabled at the Grid level and listed under the **Grid Wide** tab. You do not have to set the license at the member level.
- NIOS performs a pre-provision check for an RPZ member who joins the Grid to verify if a Grid-wide license is installed for the RPZ member. If the Grid-wide license is found, NIOS allows the member to join the Grid.
- If an RPZ license expires, Feed Zone stops receiving feed updates after the grace period. However, the RPZ feature remains active until it expires. This grace period TTL is configured in Active Trust Plus/Advanced services.
- After you remove the Grid-wide license for RPZ, this feature still keeps functioning for members that do not have a Grid-wide license until you restart the service. When you remove the RPZ license that is associated with a specific member, NIOS restarts the service automatically and disables RPZ for the respective member.
- NIOS checks for a Grid-wide license of a pre-provisioned type when a member first joins the Grid. For example, if a member is pre-provisioned for RPZ and a Grid-wide RPZ license is installed, then NIOS allows the member to join the Grid, even though the member does not have a valid RPZ license.

**Customizing Threat Feeds on an RPZ Member**

To configure an RPZ member to use your own or external threat feeds instead of RPZ feeds, complete the following:

1. From the **Data Management** tab, select **DNS**, and then click **Members**.
2. Select a member and click **Edit** from the Toolbar.
3. In the **Member DNS Properties editor**, click **General** tab -> **Advanced** tab.
   - **Apply RPZ rules only on this member if possible**: Select this check box if the forwarders must not apply RPZ rules to the responses that is returned to the other member, when this RPZ member queries other Grid member details.
4. Save the configuration.

**For FireEye Integrated RPZs**

You can enable FireEye integrated RPZs on the appliances that have both the RPZ and FireEye licenses installed. Note that you must install an RPZ license prior to installing the FireEye license.

NIOS appliance creates a new group, `fireeye-group`, when you add the first FireEye zone. The FireEye admin group is read-only and you cannot assign permissions to it. It will not have any superuser privileges and you cannot modify or delete this group. You can add users to the `fireeye-group` admin group, and FireEye users can only send alerts to the NIOS appliance. They cannot access the Infoblox GUI, CLI, API, or RESTful API. These users are authenticated based on the usernames and passwords you configure in the FireEye admin group. Only admin users who belong to the FireEye admin group can publish FireEye alerts. Other admin users cannot do so. For information about how to configure the FireEye appliance, see **Configuring the FireEye appliance**.

**Note:** The `fireeye-group` is created automatically. Infoblox recommends that you do not add a group with the same name. In addition, The “force password change at next login” feature does not apply to admin users in the `fireeye-group`. These users will not be prompted to change their passwords at the next login. Their original passwords continue to work. For more information, see **Managing Passwords**.

To add users to the `fireeye-group`, complete the following:

1. From the **Administration** tab, select **Administrators**, and then click **Admins**.
2. Click **Add** and enter the usernames and passwords. For more information on how to add users to an admin group, see **Creating Local Admins**. Select `fireeye-group` for the admin group and add users to this group.

**Note:** Ensure that you save the usernames and passwords. You must use these credentials when configuring FireEye alerts to enable the alerts to be received by NIOS.
Uninstalling the FireEye License

When you uninstall the FireEye license, new FireEye alerts will not be processed. However, the FireEye integrated RPZs and the rules in those zones will not be deleted. Note the following when you uninstall the FireEye license:

- New FireEye alerts will not be processed
- FireEye RPZ zones that were created before uninstalling the license will remain
- You cannot create new FireEye RPZ zones
- RPZ rules created from the alert will remain
- Note that if the RPZ and FireEye licenses are installed, then you must first remove the FireEye license to remove the RPZ license.
- The fireeye-group and the FireEye zones will remain even after you delete the FireEye license.

Best Practices for Configuring RPZs

Before configuring RPZs, observe the following best practices to ensure a successful configuration:

General RPZ Best Practices

- When you enable Infoblox DNS Firewall, DNS performance for all queries, recursive or authoritative, will be affected.
- For performance reasons, Infoblox recommends that you maintain a reasonable number of zones.
- Do not enable RPZ on multiple layers, such as on DNS client facing servers and forwarding.
- If you have multiple DNS servers in a Grid, ensure that you configure RPZs on the recursive server that is closest to your DNS clients. If you configure RPZs on second level DNS caching servers, you will not be able to identify the DNS clients because only the IP addresses of the forwarding name servers can be identified.
- Infoblox recommends that you preview your RPZ rules to ensure ruleset integrity and to avoid unexpected results. You can preview your rules by selecting **Log Only (Disabled)** when you configure **Policy Override** for an RPZ, RPZ feed, or FireEye integrated RPZ. For information about how to configure this, see [Configuring Local RPZs](#) and **About FireEye Integrated RPZs**.
- The appliance logs all matching and disabled rules for all queries in the syslog. You can view the syslog to ensure that the rules are set up correctly before they take effect. Ensure that you enable rpz in the **Logging Category** of Grid DNS Properties editor to log these events. For information about how to set logging categories, see [Setting DNS Logging Categories](#).
- You can use the standard TSIG mechanism to ensure that feed zones come from the correct servers. Grid members can function either as a primary or secondary servers for the RPZ. As with hosting any zone as a secondary, please ensure that the appliance is sized properly to hold the zone contents in memory.
- You can only export or import the RPZ local zones using the CSV export or import feature, but you cannot import or export FireEye zones using this feature.
- Note that the NIOS blacklist and NXDOMAIN features take precedence over RPZs.
- In order to leverage DNS notify messages to trigger zone transfer of the feed zone, port 53 of the lead secondary must be open to receive such messages. If not, the zone will refresh based on the refresh setting in the SOA.
- The name of the zone, which is assigned to an RPZ member, must not exceed 241 characters. When the name exceeds this limit, respective zone fails to load.

Best Practices For FireEye Integrated RPZs

Before you configure a FireEye integrated RPZ, consider the following:

- FireEye integrated RPZs inherit default values from local RPZs. You can create, edit and delete rules using the Infoblox GUI, API, and RESTful API.
- To avoid false positives, Infoblox recommends that you create a whitelist of allowed zones using a local RPZ that is sorted above the FireEye RPZ and add your own domain to the whitelist RPZ. For example, you can add your company domain name, such as corpxyz.com. This list must contain popular domains, such as Alexa 250, and other desired domains.
- Note that there will be an impact on the storage capacity when you create a new FireEye alert and map it with an RPZ rule. The processing of alerts will consume a few CPU cycles, which will have some impact on the system.
- You must properly configure the settings on a FireEye appliance. NIOS supports only **Per Event** delivery mechanism and JSON **Normal** message format. To ensure that the NIOS appliance process alerts properly, configure the FireEye appliance accordingly. For more information about alerts, see [Handling Alerts from the FireEye appliance](#).
- You cannot add a FireEye integrated RPZ during a scheduled full upgrade. However, updates to the CNAME record are processed during a full upgrade. NIOS updates CNAME records in the database to store information that is specific to FireEye alerts.
- The rules created due to insertion of alerts will be visible through the FireEye RPZ viewer. Infoblox recommends that you do not modify any internal objects. For more information, see [Viewing RPZs](#).
- Note that SSL certificate validation is not supported.
- You must verify the following after you configure the FireEye and NIOS appliances:
  - The URL configured on the FireEye appliance matches the URL in the FireEye integrated RPZ on NIOS.
  - Verify the username and password for FireEye admin on the FireEye appliance.
  - Ensure that the settings are properly configured on the FireEye appliance.
  - Verify the state of the FireEye appliance.
For more information about configuring the FireEye appliance to send alerts to the NIOS appliance, see Configuring the FireEye appliance.

- Note that the frequency of alerts received from FireEye can be minimal. A very small number of alerts are generated on a weekly basis. For example, the FireEye appliance may generate only tens of alerts per day.

**Enabling Recursion for RPZs**

For RPZ rules to function properly, you must enable DNS recursion. You can enable DNS recursion at the Grid, member, or DNS view level. To enable recursion:

- For the Grid or member, see Enabling Recursive Queries.
- For a DNS view, see Managing Recursive DNS Views.

**Configuring RPZs for All Recursive Servers**

When you configure a local or FireEye integrated RPZ, you must define an internal primary name server. The primary name server can be either recursive or non-recursive, depending on its usage. When you configure an RPZ feed, you must define an external primary name server. You can associate a name server or a name server group with the local RPZ, RPZ feed, or FireEye RPZ. You can also configure RPZs and RPZ feeds for all recursive servers in the Grid.

A local RPZ can have one or more secondary name servers associated with it. For an RPZ feed, you must create an external primary name server.

To configure a local RPZ, or RPZ feed, or FireEye RPZ for all recursive servers, complete the following:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then click the Add icon.
2. Enter the Response Policy Zone details and click Next to associate an RPZ with at least one name server. For information about creating a local RPZ, see Configuring Local RPZs. For information about creating an RPZ feed, see Configuring Local RPZs. For information about creating a FireEye integrated RPZ, see Configuring FireEye RPZs.
3. Select All Recursive Name Servers from the list to add all the recursive name servers in the Grid as the secondary name servers for the corresponding zone.
   - Save the configuration and click Next to define extensible attributes. Click Restart if it appears at the top of the screen. For information about extensible attributes, see About Extensible Attributes.

**Enabling and Disabling RPZ Query Name Recursion**

In previous NIOS releases, RPZ query name recursion was enabled by default. The DNS recursive name server performed RPZ recursive lookups for the fully qualified domain name that was part of an RPZ. Starting with NIOS 7.1.0, RPZ query name recursion is disabled by default.

When RPZ query name recursion is disabled, the DNS recursive name server sends responses for the domains being queried, without forwarding queries to the authoritative name servers. This can speed up recursive RPZ lookups by eliminating unnecessary recursions for domains that are known to be malicious, possibly caused by internal DDoS attacks on the recursive server.

You can enable RPZ query name recursion by selecting the Enable RPZ query name recursion (qname-wait-recurse) check box. When you select this check box, the appliance performs RPZ query name recursions. You can configure this at the Grid, member, and DNS view levels.

**Note:** RPZ query name recursion is disabled by default. The Enable RPZ query name recursion (qname-wait-recurse) check box is deselected for all new installations and upgrades. You can select this check box to enable RPZ query name recursion.

To enable or disable RPZ query name recursion:

1. From the Data Management tab, select the DNS tab, and then click Grid DNS Properties from the Toolbar.
   - or
   - From the Data Management tab, select the DNS tab -> Members tab -> Grid member check box, and then click the Edit icon.
   - or
   - From the Data Management tab, select the DNS tab -> Zones tab -> dns_view check box, and then click the Edit icon.
2. In the Grid DNS Properties, Member DNS Properties, or DNS View editor, click the General tab -> Advanced tab and complete the following.
   - Enable RPZ query name recursion (qname-wait-recurse): This check box is deselected by default, meaning RPZ query name recursion is disabled. When RPZ query name recursion is disabled, the DNS recursive name server sends responses for the domains being queried, without forwarding queries to the authoritative name servers. When you select this check box, the DNS recursive name server performs recursive lookups for the fully qualified domain names that are part of an RPZ. To override the value inherited from the Grid, click Override. To retain the same value as the Grid, click Inherit.
3. Save the configuration and click Restart if it appears at the top of the screen.

Following are sample configuration details in the named.conf file when the Enable RPZ query name recursion (qname-wait-recurse) check box is deselected:

```plaintext
response-policy {
```
1. zone "local.com" policy Given;# priority 0
2. zone "rpz.net" policy Given;# priority 1
3. zone "example.com" policy Given;# priority 2
   } qname-wait-recurse no;
   dnssec-enable yes;
   dnssec-validation yes;
   dnssec-accept-expired no;
   filter-aaaa-on-v4 no;
   zone "." in {
      type hint;
      file "named.cache._default";
   };

Configuring Local RPZs

You can define local RPZs to match responses for recursive queries. Each RPZ can have various rules associated with it. The response of a recursive query is modified if it matches any of the RPZ rules. The responses are first matched with the RPZ rules, and if there is a match, the rule defined at the RPZ level override is used. When creating a new RPZ zone, you can associate this zone with a threat severity level. The RPZ syslog messages provide information about threat severity level of an RPZ zone associated with the matched RPZ rule. To view threat details, you can drill down to the syslog messages. For more information, Viewing RPZ in the Syslog. You can create multiple local RPZs and define multiple rules for a local RPZ. Note that override depends on the order of the zones. The zones on top will override the zones below. You can change the order of the RPZs. For more information, see Reordering RPZs. You can also configure FireEye integrated RPZs on the NIOS appliance to detect persistent threats and malwares. The NIOS appliance considers the FireEye integrated RPZ as a local RPZ. For more information, see About FireEye Integrated RPZs.

Note: When using IDN (Internationalized Domain Name) in a local RPZ or RPZ feed, you must manually convert the IDN to punycode. For information about IDN, see Support for Internationalized Domain Names.

To configure local RPZs:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then click the Add icon.
2. When you click the Add icon, either the Add Response Policy Zone Wizard or the Add DNS View wizard is displayed based on the following:
   - When you click the Add icon, the Add Response Policy Zone Wizard is displayed if you have not created additional DNS views and only have the default view.

3. If you have configured multiple DNS views, you must drill-down to the corresponding view to assign a local RPZ. Click the Add icon and the Add Response Policy Zone Wizard is displayed. To create a new DNS view for your local RPZ, click the Add icon and complete the details in the Add DNS View wizard. For information, see Adding a DNS View. For information on modifying an existing view, see Modifying DNS Views.
   - In the Add Response Policy Zone Wizard, select Add Local Response Policy Zone, click Next and specify the following:
     - Name: Enter the name of the local RPZ. It can be a combination of alphanumeric characters. You can enter up to 256 characters.
     - DNS View: The name of the view that you have selected is displayed by default. You can select a view from the drop-down list to associate it with the local RPZ.

Note: The local RPZ must have a primary Grid name server before you can configure it.

- Policy Override: Select a value from the drop-down list. You can override the policy actions that are specified in the rule level.
  - Log Only (Disabled) – Select this if you want to disable an RPZ rewrite using rules in the RPZ. If the response to the recursive query matches any RPZ rule, then the rule is logged, but the response will not be altered. Note that this option will not override RPZ rules in other RPZ zones, if they take precedence. Select this option to preview the rules in the syslog before they take effect.

Note: When you select this option, the RPZ related reports are not updated, even though there is logging in the syslog.

- None (Given) – Select this if you want to use the policy from the rule level.
- Block (No Data) – Select this to send a response that contains no data in it.
- Block (No Such Domain) – Select this if you want the user to receive a DNS response that indicates there is no domain. All the policy actions in an RPZ are replaced with a NXDOMAIN block.
- Pass thru – Select this if you want to send an actual response without modification. All the policy actions in an RPZ are replaced with the passthru action.
- **Substitute (Domain Name)** – Select this if you want to replace all the policy actions in an RPZ with the specified substitution action.
  - **Domain Name**: This appears only when you select **Substitute (Domain Name)** from the Policy Override list. Enter the domain name that you want the client to receive instead of the actual domain name, which is malicious or unauthorized.
- **Severity**: Select the threat severity level for the RPZ zone. The threat severity you select here determines the severity for the RPZ zone. Select Critical, Major, Warning, or Informational. The default threat severity level is Major. Note that each of these levels is represented by a number in the syslog (8 being Critical and 4 being Informational). When you upgrade to NIOS 7.0.0, the appliance automatically updates the threat severity level to Informational (displayed as 4 in the syslog) for existing RPZ zones. For information about RPZ syslog messages and severity levels, see [Viewing RPZ in the Syslog](#).
- **Comment**: Optionally, enter additional information about the local RPZ.
- **Disable**: Select the check box to disable a local RPZ without deleting its configuration. Clear the check box to enable the local RPZ. For information, see [Enabling and Disabling Zones](#).
- **Lock**: Select the check box to lock the zone so that you can make changes to it and prevent others from making conflicting changes. For information, see [Locking and Unlocking RPZs](#).

4. Click **Next** to associate the local RPZ with at least one primary name server:

   - Define the name servers for the local RPZ. A Grid name server must be recursive when primary Grid name server is used as an RPZ source. A local RPZ may or may not have a recursive server. For example, there could be a Grid that has only primary Grid name server for a local RPZ to act as an RPZ source for an external set of name servers. A local RPZ must have only one primary Grid name server and it can have one or more secondary Grid name servers. When you select **All Recursive Name Servers** from the list, all the recursive name servers in the Grid are added as secondary servers for the zone. For information on specifying primary or secondary name server groups, see [Assigning Zone Authority to Name Servers](#). For information on specifying name server groups, see [About Name Server Groups](#). For information about all recursive name servers, see [Configuring RPZs](#) or [All Recursive Servers](#).

5. Save the configuration and click **Next** to define extensible attributes. Click **Restart** if it appears at the top of the screen. For information, see [About Extensible Attributes](#).

**Note**: You cannot convert a local RPZ to an RPZ feed or vice versa.

### Configuring Rules for RPZs

You can define different RPZ rules to block DNS resolution for malicious or unauthorized hostnames or redirect clients to a walled garden by substituting responses. Depending on the nature of the rule and its usage, each rule is designed to match a hostname, domain name, or IP address, specification or pattern, and an associated action.

These rules are applicable to local RPZs, including FireEye integrated RPZs, except for the RPZ client IP address or network rules which are not applicable for FireEye integrated RPZs. For RPZ feeds, rules are imported from external servers. You cannot change the content of an RPZ feed, but you can override the actions in an RPZ feed.

The RPZ rules are triggered based on the order of the RPZ zones that you have configured. When you configure one or more RPZ rules with the same FQDNs or IP addresses in different RPZ zones, then the RPZ rules in the top-level RPZ zone are triggered first.

**Note**: If an Infoblox-4030 appliance is already associated with a local RPZ as a Grid primary or a Grid secondary name server, then you cannot configure the client IP address or network rules for that local RPZ, and vice versa. But you can associate an Infoblox-4030 appliance with an RPZ feed, even if the RPZ feed contains client IP address or network rules.

To configure RPZ rules:

1. From the **Data Management** tab, select the **DNS** tab -> **Response Policy Zones** tab, click **DNS View** -> **Zone** and then click **Add** -> select a **Rule**.
2. The rules are classified as follows:
   - **Passthru Rule**: For information, see [Managing Passthru Rules](#).
   - **Block (No Such Domain)** Rule: For information, see [Managing Block (No Such Domain) Rules](#).
   - **Block (No Data)** Rule: For information, see [Managing Block (No Data) Rules](#).
   - **Substitute (Domain Name)** Rule: For information, see [Managing Substitute (Domain Name) Rules](#).
   - **Substitute (Record)** Rule: For information, see [Managing Substitute (Record) Rules](#).
3. Complete the details in the corresponding editor.
4. Save the configuration and click **Next** to define extensible attributes. For information about extensible attributes, see [About Extensible Attributes](#).

You cannot define the above rules for an RPZ feed. An RPZ feed uses rules defined by external servers. When you click on an RPZ feed, the appliance displays a dialog box that provides various options to export the rules of the configured external servers in .CSV format.

### Managing Passthru Rules

You can define passthru rules if you do not want to modify the actual responses of the recursive queries. The response received for a query is not modified, if there is a matching passthru rule and the actual response is forwarded to the user.
Adding Passthru Rules for Domain Names

To define passthru rules for domains:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Passthru Rule -> Passthru Domain Name Rule.
   or
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Passthru Rule -> Passthru Domain Name Rule.
2. The following fields are displayed in the Add a Passthru Domain Name Rule wizard:
   - Name: Enter the domain name for which you want to define the passthru rule. Click Select Zone to select a different zone.
   - DNS View: Displays the DNS view to which the selected RPZ belongs.
   - Policy: Displays the selected policy.
   - Comment: Optionally, enter additional information.
   - Disable: Clear the check box to enable the passthru rule. Select the check box to disable it.
3. Click Next to define extensible attributes. For information, see About Extensible Attributes.
4. Save the configuration.

Adding Passthru Rules for IP Addresses or Networks

To define passthru rules for IP addresses or networks:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Passthru Rule -> Passthru IP Address Rule.
   or
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Passthru Rule -> Passthru IP Address Rule.
2. The following fields are displayed in the Add a Passthru IP Address Rule wizard:
   - IP Address or Network: Enter the IP address or specify the address in CIDR format for which you want to define the passthru rule. Click Select Zone to select a different zone.
   - DNS View: Displays the DNS view to which the selected RPZ belongs.
   - Policy: Displays the selected policy.
   - Comment: Optionally, enter additional information.
   - Disable: Clear the check box to enable the passthru rule. Select the check box to disable it.
3. Click Next to define extensible attributes. For information, see About Extensible Attributes.
4. Save the configuration.

Adding Passthru Rules for Client IP Addresses or Networks

You can define a passthru rule for a client IP address or network, if you do not want to modify the response to a query from a specific client IP address or network and forward the actual response to the client.

To define passthru rules for the client IP addresses or networks:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Passthru Rule -> Passthru Client IP Address Rule.
   or
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Passthru Rule -> Passthru Client IP Address Rule.
2. The following fields are displayed in the Add a Passthru Client IP Address Rule wizard:
   - Client IP Address or Network: Enter the client IP address or specify the client address in CIDR format for which you want to define the passthru rule. Click Select Zone to select a different zone.
   - DNS View: Displays the DNS view to which the selected RPZ belongs.
   - Policy: Displays the selected policy.
   - Comment: Optionally, enter additional information.
   - Disable: Clear the check box to enable the passthru rule. Select the check box to disable it.
3. Click Next to define extensible attributes. For information, see About Extensible Attributes.
4. Save the configuration.

Managing Block (No Such Domain) Rules

You can define rules to block certain domain names, IP addresses or networks, or client IP addresses or networks. When you choose this option to block a domain name, the query name is matched with the RPZ rule. If the query name matches the RPZ rule, the DNS client receives a DNS response that indicates the domain does not exist.

When you block an IP address or network using this option, the A and AAAA records are matched with the RPZ rule. If the records match an RPZ rule, the DNS client receives a DNS response that indicates the domain does not exist.
When you choose this option to block a specific client IP address or network, the IP address or network of a client querying the DNS server is matched with the RPZ rule. If the IP address or the network of the client matches the RPZ rule, the DNS client receives a DNS response that indicates the domain does not exist.

**Defining Block (No Such Domain) Rules for Domain Names**

To define block rules for domains:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS View -> Zone, and then click Add -> select Block (No Such Domain) Rule -> Block Domain Name (No Such Domain) Rule.
   
   or
   
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Block (No Such Domain) Rule -> Block Domain Name (No Such Domain) Rule.

2. The following fields are displayed in the Add a Block Domain Name (No Such Domain) Rule wizard:
   - **Name**: Enter the domain name which you want to be blocked from being resolved by the DNS. Click Select Zone to select a different zone.
   - **DNS View**: Displays the DNS view to which the selected RPZ belongs.
   - **Policy**: Displays the selected policy.
   - **Comment**: Optionally, enter additional information.
   - **Disable**: Clear the check box to enable the record. Select the check box to disable it.

3. Click Next to define extensible attributes. For information, see About Extensible Attributes.

4. Save the configuration.

**Defining Block (No Such Domain) Rules for IP Addresses or Networks**

To define block rules for IP addresses or networks:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS View -> Zone, and then click Add -> select Block (No Such Domain) Rule -> Block IP Address (No Such Domain) Rule.
   
   or
   
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Block (No Such Domain) Rule -> Block IP Address (No Such Domain) Rule.

2. The following fields are displayed in the Add a Block IP Address (No Such Domain) Rule wizard:
   - **IP Address or Network**: Enter the IP address or specify the address in CIDR format which you want to block. Click Select Zone to select a different zone.
   - **DNS View**: Displays the DNS view to which the selected RPZ belongs.
   - **Policy**: Displays the selected policy.
   - **Comment**: Optionally, enter additional information.
   - **Disable**: Clear the check box to enable the block rule. Select the check box to disable it.

3. Click Next to define extensible attributes. For information, see About Extensible Attributes.

4. Save the configuration.

**Defining Block (No Such Domain) Rules for Client IP Addresses or Networks**

To define block rules for client IP addresses or networks:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS View -> Zone, and then click Add -> select Block (No Such Domain) Rule -> Block Client IP Address (No Such Domain) Rule.
   
   or
   
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Block (No Such Domain) Rule -> Block Client IP Address (No Such Domain) Rule.

2. The following fields are displayed in the Add a Block Client IP Address (No Such Domain) Rule wizard:
   - **Client IP Address or Network**: Enter the client IP address or specify the client address in CIDR format which you want to block.
     - **DNS View**: Displays the DNS view to which the selected RPZ belongs.
     - **Policy**: Displays the selected policy.
     - **Comment**: Optionally, enter additional information.
     - **Disable**: Clear the check box to enable the block rule. Select the check box to disable it.

3. Click Next to define extensible attributes. For information, see About Extensible Attributes.

4. Save the configuration.

**Managing Block (No Data) Rules**

You can define rules to block certain domain names, IP addresses or networks, or client IP addresses or networks. When you choose this option to block a domain name, the query name is matched with the RPZ rule. If the query name matches the RPZ rule, the DNS client receives a DNS response that indicates there is no data for the requested record type.
When you block an IP address or network using this option, the A and AAAA records are matched with the RPZ rules. If the records match an RPZ rule, the DNS client receives a DNS response that indicates there is no data for the requested record type.
When you choose this option to block a specific client IP address or network, the IP address or network of a client querying the DNS server is matched with the RPZ rule. If the IP address or the network of the client matches the RPZ rule, the DNS client receives a DNS response that indicates there is no data for the requested record type.

Defining Block (No Data) Rules for Domain Names

To define block rules for domains:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS View -> Zone, and then click Add -> select Block (No Data) Rule -> Block Domain Name (No Data) Rule.
   or
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Block (No Data) Rule -> Block Domain Name (No Data) Rule.
2. The following fields are displayed in the Add a Block Domain Name (No Data) Rule wizard:
   - **Name**: Enter the domain name which you want to block. Click Select Zone to select a different zone.
   - **DNS View**: Displays the DNS view to which the selected RPZ belongs.
   - **Policy**: Displays the selected policy.
   - **Comment**: Optionally, enter additional information.
   - **Disable**: Clear the check box to enable the block rule. Select the check box to disable it.
3. Click Next to define extensible attributes. For information, see About Extensible Attributes.
4. Save the configuration.

Defining Block (No Data) Rules for IP Addresses or Networks

To define block rules for IP addresses or networks:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS View -> Zone, and then click Add -> select Block (No Data) Rule -> Block IP address (No Data) Rule.
   or
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Block (No Data) Rule -> Block IP address (No Data) Rule.
2. The following fields are displayed in the Add a Block IP Address (No Data) Rule wizard:
   - **IP Address or Network**: Enter the IP address or specify the address in CIDR format which you want to block. Click Select Zone to select a different zone.
   - **DNS View**: Displays the DNS view to which the selected RPZ belongs.
   - **Policy**: Displays the selected policy.
   - **Comment**: Optionally, enter additional information.
   - **Disable**: Clear the check box to enable the block rule. Select the check box to disable it.
3. Click Next to define extensible attributes. For information, see About Extensible Attributes.
4. Save the configuration.

Defining Block (No Data) Rules for Client IP Addresses or Networks

To define block rules for client IP addresses or networks:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS View -> Zone, and then click Add -> select Block (No Data) Rule -> Block Client IP address (No Data) Rule.
   or
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Block (No Data) Rule -> Block Client IP address (No Data) Rule.
2. The following fields are displayed in the Add a Block Client IP Address (No Data) Rule wizard:
   - **Client IP Address or Network**: Enter the client IP address or specify the client address in CIDR format which you want to block. Click Select Zone to select a different zone.
   - **DNS View**: Displays the DNS view to which the selected RPZ belongs.
   - **Policy**: Displays the selected policy.
   - **Comment**: Optionally, enter additional information.
   - **Disable**: Clear the check box to enable the block rule. Select the check box to disable it.
3. Click Next to define extensible attributes. For information, see About Extensible Attributes.
4. Save the configuration.

Managing Substitute (Domain Name) Rules

You can define an alternate IP address or a domain name to redirect a domain name or an IP address, which is malicious or unauthorized. When the response to the client query matches an RPZ rule, the actual domain name or IP address is substituted with the alternative domain name or IP address.
Defining Substitute Domain Name (Based on Domain Name) Rules

To define substitutes for domain names:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Substitute (Domain Name) Rule -> Substitute Domain Name (Domain Name) Rule.
   
   or
   
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Substitute (Domain Name) Rule -> Substitute Domain Name (Domain Name) Rule.
   
2. The following fields are displayed in the Add a Substitute (Domain Name) Rule wizard:
   - Name: Enter the domain name for which you want to define a substitute. Click Select Zone to select a different zone.
   - DNS View: Displays the DNS view to which the selected RPZ belongs.
   - Policy: Displays the selected policy.
   - Substituted Name: Enter an alternative domain name or IP address that has to be substituted with the actual domain name.
   - Comment: Optionally, enter additional information.
   - Disable: Clear the check box to enable the substitute rule. Select the check box to disable it.
   
3. Click Next to define extensible attributes. For information, see About Extensible Attributes.
4. Save the configuration.

Defining Substitute Domain Name (Based on IP address) Rules

To define substitutes for IP addresses:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Substitute (Domain Name) Rule -> Substitute Domain Name (IP Address) Rule.
   
   or
   
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Substitute (Domain Name) Rule -> Substitute Domain Name (IP Address) Rule.
   
2. The following fields are displayed in the Add a Substitute Domain Name (IP Address) Rule wizard:
   - IP address or Network: Enter the IP address or network for which you want to define a substitute. Click Select Zone to select a different zone.
   - DNS View: Displays the DNS view to which the selected RPZ belongs.
   - Policy: Displays the selected policy.
   - Substituted Name: Enter an alternative domain name or IP address that has to be substituted with the actual IP address.
   - Comment: Optionally, enter additional information.
   - Disable: Clear the check box to enable the substitute rule. Select the check box to disable it.
   
3. Click Next to define extensible attributes. For information, see About Extensible Attributes.
4. Save the configuration.

Defining Substitute Domain Name (Based on Client IP address) Rules

You can define a substitute domain name rule for a client IP address if you want to substitute the actual response to a query from the DNS client with an alternate domain name or IP address. When the IP address of the client querying a DNS server matches the RPZ rule, the actual response is substituted with the alternative domain name or IP address specified in the RPZ rule.

To define substitute domain name rule for client IP addresses:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Substitute (Domain Name) Rule -> Substitute Domain Name (Client IP Address) Rule.
   
   or
   
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Substitute (Domain Name) Rule -> Substitute Domain Name (Client IP Address) Rule.
   
2. The following fields are displayed in the Add a Substitute Domain Name (Client IP Address) Rule wizard:
   - Client IP address or Network: Enter the client IP address or client network for which you want to define a substitute domain name (client IP address) rule. Click Select Zone to select a different zone.
   - DNS View: Displays the DNS view to which the selected RPZ belongs.
   - Policy: Displays the selected policy.
   - Substituted Name: Enter an alternative domain name or IP address that replaces the actual DNS response. Click Select Zone t
To define substitute rules for AAAA records:

An RPZ AAAA (address) record maps a domain name to a substitute IPv6 address. To define a specific name-to-address mapping, add an AAAA record to a previously defined RPZ.

To define substitute rules for AAAA records:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Substitute (Record) Rule -> Substitute (AAAA Record) Rule.

2. The following fields are displayed in the Add a Substitute (AAAA Record) Rule wizard:
   - Name: Enter the domain name that you want to map to an IPv6 address. The name that you specify, irrespective of the RPZ name, is used to determine a match for the RPZ rule. Click Select Zone to select a different zone.
   - DNS View: Displays the DNS view to which the selected RPZ belongs.
   - IP Address: Enter the IPv6 address to which you want the domain name to map.
   - Comment: Optionally, enter additional information about the AAAA record.
   - Disable: Clear the check box to enable the record. Select the check box to disable it.

3. Click Next to define extensible attributes. For information, see About Extensible Attributes.

4. Save the configuration.

Managing Substitute (Record) Rules

You can define a substitute record for a domain name, which is considered malicious. You can define substitutes for the following in a zone:

- A records: For information about defining substitutes for A records, see Defining Substitutes Rules for A Records.
- AAAA records: For information about defining substitutes for AAAA records, see Defining Substitute Rules for AAAA Records.
- MX records: For information about defining substitutes for MX records, see Defining Substitute Rules for MX Records.
- NAPTR records: For information about defining substitutes for NAPTR records, see Defining Substitute Rules for NAPTR Records.
- PTR records: For information about defining substitutes for PTR records, see Defining Substitute Rules for PTR Records.
- SRV records: For information about defining substitutes for SRV records, see Defining Substitute Rules for SRV Records.
- TXT records: For information about defining substitutes for TXT records, see Defining Substitute Rules for TXT Records.
- IPv4 addresses: For information about defining substitutes for IPv4 addresses, see Defining Substitute Rules for IPv4 Addresses or Networks.
- IPv6 addresses: For information about defining substitutes for IPv6 addresses, see Defining Substitute Rules for IPv6 Addresses or Networks.

You can define a substitute for a certain owner name and record type. When you substitute a record for a certain owner name and record type, then responses to queries for that owner name and type are modified to contain the substituted value(s).

Defining Substitutes Rules for A Records

An RPZ A (address) record maps a domain name to a substitute IPv4 address. To define a specific name-to-address mapping, add an A record to a previously defined RPZ.

To define substitute rules for A records:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Substitute (Record) Rule -> Substitute (A Record) Rule. or

2. The following fields are displayed in the Add a Substitute (A Record) Rule wizard:
   - Name: Enter the domain name that you want to map to an IP address. The name that you specify, irrespective of the RPZ name, is used to determine a match for the RPZ rule. Click Select Zone to select a different zone.
   - DNS View: Displays the DNS view to which the selected RPZ belongs.
   - IP Address: Enter the IPv4 address to which you want the domain name to map.
   - Comment: Optionally, enter additional information about the A record.
   - Disable: Clear the check box to enable the record. Select the check box to disable it.

3. Click Next to define extensible attributes. For information, see About Extensible Attributes.

4. Save the configuration.

Defining Substitute Rules for AAAA Records

An RPZ AAAA (address) record maps a domain name to a substitute IPv6 address. To define a specific name-to-address mapping, add an RPZ AAAA record to a previously defined RPZ.

To define substitute rules for AAAA records:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Substitute (Record) Rule -> Substitute (AAAA Record) Rule.

2. The following fields are displayed in the Add a Substitute (AAAA Record) Rule wizard:
   - Name: Enter the domain name that you want to map to an IPv6 address. The name that you specify, irrespective of the RPZ name, is used to determine a match with the RPZ rule. Click Select Zone to select a different zone.
   - DNS View: Displays the DNS view to which the selected RPZ belongs.
   - IP Address: Enter the IPv6 address to which you want the domain name to map.
   - Comment: Optionally, enter additional information about the AAAA record.
   - Disable: Clear the check box to enable the record. Select the check box to disable it.

3. Click Next to define extensible attributes. For information, see About Extensible Attributes.

4. Save the configuration.

Copyright ©2019, Infoblox, Inc. All right reserved.
Defining Substitute Rules for MX Records

An RPZ MX (mail exchanger) record maps a domain name to a mail exchanger. A mail exchanger is a server that either delivers or forwards mail. A wildcard MX record applies to an RPZ and all its subdomains of the owner name.

To define substitute rules for MX records:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Substitute (Record) Rule -> Substitute (MX Record) Rule.
   
or
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Substitute (Record) Rule -> Substitute (MX Record) Rule.

2. The following fields are displayed in the Add a Substitute (MX Record) Rule wizard:
   - **Mail Destination:** Enter the owner name of the MX record you want to substitute.
   - **DNS View:** Displays the DNS view to which the selected RPZ belongs.
   - **Host Name Policy:** Displays the hostname policy of the selected zone. Ensure that the hostname you enter complies with the hostname restriction policy defined for the zone.
   - **Mail Exchanger:** Enter the fully qualified domain name of the mail exchanger.
   - **Preference:** Select an integer from 10 to 100. The preference determines the order in which a client attempts to contact the target mail exchanger.
   - **Comment:** Optionally, enter additional information about the MX record.
   - **Disable:** Clear the check box to enable the record. Select the check box to disable it.

3. Click Next to define extensible attributes. For information, see About Extensible Attributes.

4. Save the configuration.

Defining Substitute Rules for NAPTR Records

A DNS NAPTR object represents a Naming Authority Pointer (NAPTR) resource record. This resource record specifies a regular expression-based rewrite rule that, when applied to an existing string, produces a new RPZ name or URI.

To define substitute rules for NAPTR records:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Substitute (Record) Rule -> Substitute (NAPTR Record) Rule.
   
or
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Substitute (Record) Rule -> Substitute (NAPTR Record) Rule.

2. The following fields are displayed in the Add a Substitute (NAPTR Record) Rule wizard:
   - **Domain:** Enter the domain name to which this resource record refers. Make sure that you enter a valid FQDN. Example: test.com, foo.com, etc. The name that you specify, irrespective of the RPZ name, is used to determine a match with the RPZ rule. Click Select Zone to select a different zone.
   - **DNS View:** Displays the DNS view to which the selected RPZ belongs.
   - **Service:** Select a service from the drop-down list. This field specifies the service and protocol that are used to communicate with the host at the domain name.
   - **Flags:** The Flag field indicates whether the current lookup is terminal; that is, the current NAPTR record is the last NAPTR record for the lookup. It also provides information about the next step in the lookup process. The flags that are currently used are:
     - **U:** Indicates that the output maps to a URI (Uniform Record Identifier).
     - **S:** Indicates that the output is a domain name that has at least one SRV record. The DNS client must then send a query for the SRV record of the resulting domain name.
     - **A:** Indicates that the output is a domain name that has at least one A or AAAA record. The DNS client must then send a query for the A or AAAA record of the resulting domain name.
     - **P:** Indicates that the protocol specified in the Service field defines the next step or phase.
   - **Order:** Select an Integer from 10 to 100, or enter a value from 0 to 65535. This value indicates the order in which the NAPTR records must be processed. It processes the record with the lowest value first.
   - **Preference:** Select an Integer from 10 to 100, or enter a value from 0 to 65535. Similar to the Preference field in MX records, this value indicates which NAPTR record the DNS client should process first when the records have the same Order values. It processes the record with the lowest value first.
   - **REGEFX:** The regular expression that is used to rewrite the original string from the client into a domain name. RFC 2915 specifies the syntax of the regular expression. Note that the appliance validates the regular expression syntax between the first and second delimiter against the Python re module, which is not 100% compatible with POSIX Extended Regular Expression as specified in the RFC. For information about the Python re module, refer to [http://docs.python.org/release/2.5.1/lib/module-re.html](http://docs.python.org/release/2.5.1/lib/module-re.html).
   - **Replacement:** This specifies the domain name for the next lookup. The default is a dot (.), which indicates that the regular expression in the REGEX field provides the replacement value. Alternatively, you can enter the replacement value in FQDN format.
   - **Comment:** Optionally, enter additional information about the NAPTR record.
   - **Disable:** Clear the check box to enable the record. Select the check box to disable it.

3. Click Next to define extensible attributes. For information, see About Extensible Attributes.

4. Save the configuration.
Defining Substitute Rules for PTR Records

In a forward-mapping zone, a PTR (pointer) record maps a domain name to another domain name. In an RPZ, a PTR (pointer) record maps an address to a domain name. To define a specific address-to-name mapping, add an RPZ PTR record to a previously defined RPZ.

To define substitute rules for PTR records:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Substitute (Record) Rule -> Substitute (PTR Record) Rule.
   
   or
   
   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Substitute (Record) Rule -> Substitute (PTR Record) Rule.

2. The following fields are displayed in the Add a Substitute (PTR Record) Rule wizard: You can select either Name or IP address from the drop-down list.
   - **Name:** Enter a domain name for which you want to create a pointer to another domain. The name that you specify, irrespective of the RPZ name, is used to determine a match with the RPZ rule. Click Select Zone to select a different zone. The name should be in the following format for RPZ:
     
     ipaddress.in-addr.arpa.
     
     Note that the IP address should be in the reverse format. For example, if the IP address is 10.2.1.4, then the name format for RPZ is 4.1.2.10.in-addr.arpa. The following fields are displayed when you select Name from the drop-down list:
     
     - **DNS View:** Displays the DNS view to which the selected RPZ belongs.
     - **Domain Name:** Enter the domain name to which you want the PTR record to point. Make sure that you enter a valid FQDN. Example: test.com, foo.com, etc.
     - **IP Address:** Enter an IP address for which you want to create a pointer to a domain. The following fields are displayed when you select IP Address from the drop-down list:
       
       - **Zone:** Displays the RPZ you have selected. Click Select Zone to select a different zone.
       - **DNS View:** Displays the DNS view to which the selected RPZ belongs.
       - **Domain Name:** Enter the domain name to which you want the PTR record to point. Make sure that you enter a valid FQDN. Example: test.com, foo.com, etc.
       - **Comment:** Optionally, enter additional information about the PTR record.
     - **Disable:** Clear the check box to enable the record. Select the check box to disable it.

3. Click Next to define extensible attributes. For information, see About Extensible Attributes.

4. Save the configuration.

Defining Substitute Rules for SRV Records

A DNS RPZ SRV object represents an SRV resource record, which is also known as a service record. You can define a substitute for an SRV record. When the response to a user's query matches with an RPZ rule, then the combination of actual service, protocol, domain name and the zone is substituted with a combination of priority, weight, port and target details that you specify.

To define substitute rules for SRV records:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Substitute (Record) Rule -> Substitute (SRV Record) Rule.

   or

   From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Substitute (Record) Rule -> Substitute (SRV Record) Rule.

2. The following fields are displayed in the Add a Substitute (SRV Record) Rule wizard:
   - **Display input as:** Select the format in which you want the SRV record to be displayed. When you select RFC 2782 format, the appliance follows the _service._protocol.name format as defined in RFC 2782. When you select Free format, enter the entire name in the Domain field.
   - **Service:** Specify the service that the host provides. You can either select a service from the list or type in a service. If it is not on the list. For example, if you are creating a record for a host that provides FTP service, select _ftp. To distinguish the service name labels from the domain name, the service name is prefixed with an underscore. If the name of the service is defined in RFC 1700, Assigned Numbers, use that name. Otherwise, you can use a locally-defined name. This field is disabled when you select Free Format as the display input.
   - **Protocol:** Specify the protocol that the host uses. You can either select a protocol from the list or type in a protocol. If it is not on the list. For example, if it uses TCP, select _tcp. To distinguish the protocol name labels from the domain name, the protocol name is prefixed with an underscore. This field is disabled when you select Free Format as the display input.
   - **Domain:** If Grid Manager displays a zone name, enter the name here to define an SRV record for a host or subdomain. The displayed zone name can either be the last selected zone or the zone from which you are adding the SRV record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the ZoneSelector dialog box. Click a zone name in the dialog box, and then enter the name to define the SRV record. The SRV record name is used to determine the substitute.
   - **Preview:** After you enter all the information, this field displays the FQDN.
   - **DNS View:** Displays the DNS view to which the selected RPZ belongs.
   - **Priority:** Select or enter an integer from 0 to 65535. The priority determines the order in which a client attempts to contact the target host; the domain name host with the lowest number has the highest priority and is queried first. Target hosts with the same priority are attempted in the order defined in the Weight field.
Defining Substitute Rules for TXT Records

A TXT (text) record contains supplemental information for a host. SPF (Sender Policy Framework) records are specialized RPZ TXT records that identify the servers that send mail from a domain.

To define substitute rules for TXT records:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS View -> Zone, and then click Add -> select Substitute (Record) Rule -> Substitute (TXT Record) Rule.

2. The following fields are displayed in the Add a Substitute (TXT Record) Rule wizard:
   - Name: Enter the name to define a TXT record for a host or subdomain. The name that you specify, irrespective of the RPZ name, is used to determine a match with the RPZ rule. Click Select Zone to select a different zone.
   - DNS View: Displays the DNS view to which the selected RPZ belongs.
   - Text: Enter the text that you want to associate with the record. It can contain substrings of up to 255 bytes, up to a total of 512 bytes. Additionally, if you enter leading, trailing, or embedded spaces in the text, add quotes around the text to preserve the spaces. For example: " v=spf1 include:corp200.com -all ".
   - Comment: Optionally, enter additional information about the TXT record.
   - Disable: Clear the check box to enable the record. Select the check box to disable it.

3. Click Next to define extensible attributes. For information, see About Extensible Attributes.

4. Save the configuration.

Defining Substitute Rules for IPv4 Addresses or Networks

You can define a substitute for an IPv4 address or a network address. When a client queries for A records of a domain name, if the IP address in A records in the response match the specified address or network, then the response is modified to instead contain the substituted address.

To define substitute rules for IPv4 addresses or networks:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS View -> Zone, and then click Add -> select Substitute (Record) Rule -> Substitute (IPv4 Address) Rule.

2. The following fields are displayed in the Add a Substitute (IPv4 Address) Rule wizard:
   - IP Address or Network: Enter the IPv4 address which you want to substitute with another IPv4 address. Click Select Zone to select a different zone.

3. Click Next to define extensible attributes. For information, see About Extensible Attributes.

4. Save the configuration.

Defining Substitute Rules for IPv6 Addresses or Networks

You can restrict access to specific IPv6 addresses or networks by providing a substitute IP address. When a client queries for AAAA records of a domain name if the IP addresses in AAAA records in the response match the specified address or network, then the response is modified to instead contain the substituted address.

Note: You cannot define a substitute rule for the same IP address or a network address for which you have already defined a passthru rule.

- DNS View: Displays the DNS view to which the selected RPZ belongs.
- Policy: Displays the selected policy.
- Substituted IP Address: Enter the IPv4 address that must be returned to the user when the response matches the A records.
- Comment: Optionally, enter additional information about the IPv4 address.
- Disable: Clear the check box to enable the record. Select the check box to disable it.

3. Click Next to define extensible attributes. For information, see About Extensible Attributes.

4. Save the configuration.
To define substitute rules for IPv6 addresses or networks:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, select DNS_View -> Zone, and then click Add -> select Substitute (Record) Rule -> Substitute (IPv6 Address) Rule.
   or From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then select a zone. Expand the Toolbar, click Add -> select Substitute (Record) Rule -> Substitute (IPv6 Address) Rule.
2. The following fields are displayed in the Add a Substitute (IPv6 Address) Rule wizard:
   - **IP Address or Network:** Enter the IPv6 address or the network address which you want to substitute with another IP address.
   - **DNS View:** Displays the DNS view to which the selected RPZ belongs.
   - **Policy:** Displays the selected policy.
   - **Substituted IP Address:** Enter the IPv6 address that must be returned to the user when the response matches the AAAA records.
   - **Comment:** Optionally, enter additional information about the IPv6 address.
   - **Disable:** Clear the check box to enable the record. Select the check box to disable it.
3. Click Next to define extensible attributes. For information, see About Extensible Attributes.
4. Save the configuration.

### Configuring Infoblox Threat Intelligence Feed

Starting with NIOS 7.3.200, Infoblox introduces the Infoblox Threat Intelligence Feed, a threat feed subscription for RPZ updates that offer protection against malicious hostnames. Contact your Infoblox representative for pricing and availability information.

When you upgrade from a previous NIOS release to NIOS 7.3.200 and later releases, the Infoblox RPZ feeds you configured in the previous NIOS release are migrated to the upgraded release. For information about the old RPZ feeds, refer to the NIOS 7.3.4 and earlier NIOS Administor Guides.

You can configure the Threat Intelligence Feed and receive reputation RPZ updates on a regular basis. An RPZ feed receives response policies from the Infoblox in-house threat intelligence team, which produces reputation RPZ data and transfers the data to Grid name servers through zone transfers with or without a TSIG key. To ensure proper authentication and integrity of the RPZ feed zone transfers, using a TSIG key is recommended.

**Note:** TSIG Key is used for authentication when downloading information about threat protection feeds. If you have a complex configuration, such as using standalone appliances or Grids that receive threat protection feeds from other standalone appliances or Grids and not directly from the Infoblox distribution servers, ensure that you use the same TSIG key for the RPZ feed zone transfers.

Note that the RPZ feed must have an external primary name server before you can configure it. To propagate RPZs as quickly as possible, the secondary DNS server needs an address to which the RPZ source feed can send NOTIFY messages. For example, if the secondary DNS server is configured behind a NAT, you may want to establish a one-to-one NAT for the lead secondary DNS server so it can receive NOTIFY messages from the RPZ source feed. Otherwise, the lead secondary DNS server will need to periodically poll the RPZ source feed, which could take longer than expected.

**Note:** To enter IDNs (Internationalized Domain Name) in an RPZ feed, you can use the punycode representation of the IDN.

To configure the Threat Intelligence Feed:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then click the Add icon.
2. When you click the Add icon, either the Add Response Policy Zone Wizard or the Add DNS View wizard is displayed based on the following:
   - When you click the Add icon, the Add Response Policy Zone Wizard is displayed, if you have not created additional DNS views and only have the default view.
   - If you have configured multiple DNS views, you must drill-down to the corresponding DNS_View to assign an RPZ feed. Click the Add icon and the Add Response Policy Zone Wizard is displayed. To create a new DNS view for your RPZ feed, click the Add icon, and complete the details in the Add DNS View wizard. For information, see Configuration Example: Configuring a DNS View. For information on modifying an existing view, see Modifying DNS Views.
3. In the Add Response Policy Zone Wizard, select Add Response Policy Zone Feed, click Next and specify the following:
   - **Name:** Enter the name of the Infoblox RPZ feed. It can be a combination of alphanumeric characters. You can enter up to 256 characters. For more information, see Infoblox Threat Intelligence Feeds.
   - **DNS View:** The name of the view that you have selected is displayed by default. You can select a view from the drop-down list to associate it with the RPZ feed.
   - **Policy Override:** Select a value from the drop-down list. You can override the policy actions that are specified in the rule level.
     - **Log Only (Disabled)** — Select this if you want to disable an RPZ rewrite using rules in the RPZ zone. If the response to the recursive query matches any RPZ rule, the rule is logged, but the response will not be altered. You cannot overwrite the response to the user. Note that this option will not override RPZ rules in other RPZ zones, if they take precedence.
     - **None (Given)** — Select this if you want to use the policy from the rule level.
     - **Block (No Data)** — Select this if you want the user to receive a response that indicates that there is no data.
     - **Block (No Such Domain)** — Select this if you want the user to receive a NXDOMAIN as the DNS response. All the policy actions in an RPZ are replaced with a NXDOMAIN block.
     - **Passthru** — Select this if you want the user to see the actual response without modification. All the policy actions in an RPZ are replaced with the passthru action.
• **Substitute (Domain Name)** – Select this if you want to replace all the policy actions in an RPZ with the substitution action that is specified.
  • **Domain Name**: This appears only when you select **Substitute (Domain Name)** from the **Policy Override** list. Enter the domain name that you want the client to receive instead of the actual domain name, which is malicious or unauthorized.

• **Severity**: Select the threat severity level for the RPZ zone. The threat severity you select here determines the severity for the RPZ rule. Select **Critical**, **Major**, **Warning**, or **Informational**. The default threat severity level is Major. Note that each of these levels is represented by a number in the syslog (8 being Critical and 4 being Informational). When you upgrade to NIOS 7.0.0, the appliance automatically updates the threat severity level to Informational (displayed as 4 in the syslog) for existing RPZ zones. For information about RPZ syslog messages and severity levels, see **Viewing RPZ in the Syslog**.

• **Comment**: Optionally, enter additional information about the Infoblox RPZ feed.

• **Disable**: Select the check box to disable the RPZ feed without deleting its configuration. Clear the check box to enable the RPZ feed. For information, see **Enabling and Disabling Zones**.

• **Lock**: Select the check box to lock the RPZ feed so that you can make changes to it and prevent others from making conflicting changes. For information, see **Locking and Unlocking RPZs**.

4. Click **Next** to associate the RPZ feed with at least one external primary name server and a secondary name server:

• Define name servers for the RPZ feed. An RPZ feed must have at least one RPZ source as an external primary name server and at least one Grid secondary name server. For external primary servers, specify the following:
  • **Name**: Enter the zone name of the primary name server.
  • **Address**: Enter the name server IP address provided by Infoblox for the RPZ feed.
  • **Use TSIG**: Select the check box to specify TSIG settings.
  • **Key Name**: Enter the TSIG Key Name provided by Infoblox.
  • **Algorithm**: Select `hmac-md5`.
  • **Key Data**: Enter the TSIG string provided by Infoblox.
  Note that either the Grid name server or the DNS view must be recursive for the RPZ feed. You can associate a lead secondary with an RPZ feed. For information on specifying primary and secondary, see **Assigning Zone Authority to Name Servers**. When you select **All Recursive Name Servers** from the list, all the recursive name servers in the Grid are added as secondary servers for the zone. For information about all recursive name servers, see **Configuring RPZs for All Recursive Servers**. For information on specifying name server groups, see **About Name Server Groups**.

5. Save the configuration and click **Next** to define extensible attributes. Click **Restart** if it appears at the top of the screen. For information, see **About Extensible Attributes**.

**Infoblox Threat Intelligence Feeds**

Infoblox RPZ feeds are categorized into pure malicious feeds and combination feeds. All the feeds listed below are set to return NXDOMAIN for items in the feed. Threat data changes are pushed every 20 minutes from the DNS servers and significant changes are typically made every two hours.

The following tables list the Infoblox Threat Intelligence feeds:

**Table 42.1 Pure Malicious Feeds**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base (base.rpz.infoblox.local)</td>
<td>Enables protection against known hostnames that are dangerous as destinations, such as APT, Bot, Compromised Host/Domains, Exploit Kits, Malicious Name Servers, and Sinkholes along with bogon IP addresses.</td>
</tr>
<tr>
<td>AntiMalware (antimalware.rpz.infoblox.local)</td>
<td>Enables protection against known malicious threats that can take action on or control of your system, such as Malware Command &amp; Control, Malware Download, and active Phishing sites.</td>
</tr>
<tr>
<td>Ransomware (ransomware.rpz.infoblox.local)</td>
<td>Enables protection against ransomware that restricts access to the computer system that it infects, and demands a ransom paid to the creator of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive, while some may simply lock the system and display messages intended to coax the user into paying. Examples include Locky, CryptoLocker, Dircrypt, and CryptoWall.</td>
</tr>
<tr>
<td>Bogon (bogon.rpz.infoblox.local)</td>
<td>Enables protection against bogons, which are commonly found as the source addresses of DDoS attacks. A bogon is an informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved, but not yet allocated or delegated by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). The areas of unallocated address space are called bogon space. Many ISPs and end-user firewalls filter and block bogons, because they have no legitimate use, and usually are the result of accidental or malicious misconfiguration.</td>
</tr>
</tbody>
</table>
AntiMalware_IP (antimalware-ip.rpz.infoblox.local) Enables protection against known malicious or compromised IP addresses. These are known to host threats that can take action on or control of your system, such as Malware Command & Control, Malware Download, and active Phishing sites.

Bot_IP (bot-ip.rpz.infoblox.local) Enables protection against self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet." With a botnet, attackers can launch broad-based, "remote-control," flood-type attacks against their target(s). Bots can also log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch DoS attacks, relay spam, and open back doors on the infected host.

ExploitKit_IP (exploitkit-ip.rpz.infoblox.local) Enables protection against distributable packs that contains malicious programs that are used to execute "drive-by-download" attacks in order to infect users with malware. These exploit kits target vulnerabilities in the users' machines (usually due to unpatched versions of Java, Adobe Reader, Adobe Flash, Internet Explorer, ...) to load malware onto the victim's computer.

Malware_DGA (malware-dga.rpz.infoblox.local) Domain generation algorithm (DGA) are algorithms seen in various families of malware that are used to periodically generate a large number of domain names that can be used as rendezvous points with their command and control servers. Examples include Ramnit, Conficker, and Banjoni.

TOR_Exit_Node_IP (tor-exit-node-ip.rpz.infoblox.local) Tor Exit Nodes are the gateways where encrypted Tor traffic hits the Internet. This means an exit node can be used to monitor Tor traffic (after it leaves the onion network). It is in the design of the Tor network that locating the source of that traffic through the network should be difficult to determine.

SURBL_Multi (multi-domain.surbl.rpz.infoblox.local) Blacklist of Malicious Domains including up-to-date intel on active malware, phishing, botnet, and spam domains. Based on data provided by our partner SURBL.

SURBL_Fresh (fresh-domain.surbl.rpz.infoblox.local) Newly Observed Domains. SURBL Fresh feed provides critical, accurate, information on the time new domains are placed into service. Security policy can be easily applied (block, quarantine, walled garden, etc.) to prevent resolution of new domains, based on the user's defined policies. Based on data provided by our partner SURBL.

### Downloading Rules for an RPZ Feed

You can perform a zone transfer to transfer the rules from an external primary name server to the RPZ feed. You cannot modify these rules, but you can override the entire ruleset or an individual rule. However, if you import a zone to a local zone, you can edit the rules within a local zone. The feed zone supports NSIP and NSDNAME rules; however local RPZs do not support these rules. To download rules from an external primary name server:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then click the corresponding RPZ Feed.
2. In the Export dialog box, complete the following:
   - Separator: Select the separator used in the data file. The default value is Comma.
   - Click Export.

All the rules are transferred. You can download rules only if the lead secondary has completed at least one zone transfer from the external primary. You can either open the data file or save it to your computer. The rules are displayed for the selected RPZ feed in the Rule wizard. After you have downloaded rules from an RPZ feed, you can test RPZ feed policies, as described in Testing RPZ Feed Rules.

### Testing RPZ Feed Rules

After you have downloaded rules from an RPZ feed, you can test the downloaded policies by using the dig command and observing log messages that contain redirect or rewrite responses in the syslog. The NIOS appliance supports generation of RPZ log messages in CEF (Common Event Format). Note that non-RPZ messages cannot be generated in CEF.

You must enable the rpz option in the Logging Category of the Grid DNS Properties editor to receive RPZ related messages in the syslog. For information about configuring the logging category, see Setting DNS Logging Categories.

To view RPZ log messages in the syslog, you can use the system filter RPZ Logs from the Quick Filter to filter the messages. Note that only messages in CEF are displayed.

To view RPZ log messages:

1. From the Administration tab, select the Logs tab -> Syslog tab.
2. From the drop-down list at the upper right corner, select the Grid member on which you want to view the syslog.
3. Click Show Filters to enable the filters. Select RPZ Logs from the Quick Filter drop-down list to narrow down the system messages you want to view.

The name server recursive cache makes a syslog entry when an RPZ functionality fails. The syslog message log format is as follows:

```
rpz <TYPE> rewrite <QUERY> via <RPZ_RECORD><ERROR_MESSAGE>
```

where: <TYPE> is one of following RPZ action types: QNAME, IP, NSIP, NSDNAME, CLIENT-IP;
<QUERY> is a query record to process;
<RPZ_RECORD> is an RPZ record that is used to perform an action to the query;
<ERROR_MESSAGE> is a message with error details. Example: NS address rewrite rrset failed:, concatenate() failed:, NS db_find() failed:, stop on qresult in rpz_rewrite() failed:, stop on unrecognized qresult in rpz_rewrite() failed:, etc.

To test RPZ feed policies:

1. Open a terminal console on your computer.
2. Type the command `dig @<your DNS server IP> <queried domain>`.
3. Go to the Administration tab -> Logs tab -> Syslog tab to view CEF log messages.

About FireEye Integrated RPZs

Infoblox DNS Firewall provides a mechanism to further protect your network from malware and APTs (Advanced Persistent Threats) through the integration of FireEye appliances. When your NIOS appliance is properly integrated with a FireEye appliance, it receives periodic alerts and APTs from the FireEye appliance when it identifies such threats. Based on your configuration, the NIOS appliance translates these alerts into RPZ rules that not only further protect your network from malicious attacks, but also aid in identifying clients that have been compromised.

As illustrated in Figure 42.2, after installing the required RPZ and FireEye licenses on the NIOS appliance, you can configure a FireEye integrated RPZ in which you map RPZ rules to FireEye alert types. While creating the FireEye RPZ, the appliance generates a URL to which the FireEye appliance sends alerts. Ensure that you enter this URL when configuring the FireEye appliance. The NIOS appliance also creates the fireeye-group admin group after you define the first FireEye RPZ. You can add multiple admin users to this admin group. Note that users in the fireeye-group can only send alerts to the NIOS appliance; they cannot access the Infoblox GUI, CLI, API and RESTful API. They also do not have permissions to perform other tasks on the appliance. Ensure that you record the usernames and passwords for all user accounts so you can enter them correctly when you configure the FireEye appliance. You can map a single or multiple FireEye appliances to a NIOS appliance where multiple users or zones exist.

To configure a FireEye integrated RPZ, complete the following:

1. Create a new FireEye integrated RPZ, as described in Configuring FireEye RPZs.
2. Create FireEye admin users, as described in FireEye Integrated RPZs.
3. Add URL and user credentials on the FireEye appliance, as described in Configuring the FireEye appliance.
4. When a malware or threat is detected, the FireEye appliance sends an alert message to the NIOS appliance, which is stored in the syslog. For more information, see Handling Alerts from the FireEye appliance.

Configuring FireEye RPZs

You must create an RPZ zone and map the FireEye alerts with an RPZ rule to receive alerts from FireEye. These alerts will then be translated into appropriate RPZ rules that are added to the FireEye RPZ. You can also define a time limit for a specific alert type or set the alert type to live forever. When you define a lifetime, the alert type will be active for the specified number of days or weeks in the NIOS appliance, and will then expire after the specified time. After you configure the FireEye integrated RPZ, the NIOS Grid receives alerts from the FireEye appliance and creates RPZ rules for some of the alerts received. FireEye appliance sends alert messages with basic authentication. You must configure a username and password on the NIOS appliance prior to receiving any alerts from the FireEye appliance.

Note: The NIOS appliance treats the FireEye integrated RPZ as a local RPZ. Thus, you cannot assign an external primary name server to the zone.

An alert contains the malware URL along with a valid FQDN. The NIOS appliance can only map an alert to a RPZ rule if the FQDN is present. If an alert doesn’t contain the FQDN, then the alert is ignored by the NIOS appliance. For more information about alerts, see Handling Alerts from the FireEye appliance. Once the alert is processed and properly mapped to an RPZ rule, it remains in the database until you delete it manually. You
can get more information about the alerts, which are sent by the FireEye appliance, from the syslog.

**Note:** You can configure feeds from multiple FireEye appliances. To enable or disable FireEye integration module feeds from individual appliances, you must enable or disable user access of the particular FireEye appliance. Note that the FireEye feeds will not be in the RPZ format, but when you configure a FireEye integrated RPZ, the NIOS appliance creates a new URL through which the FireEye appliance sends alerts.

To configure a FireEye integrated RPZ:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, and then click the Add icon.
2. When you click the Add icon, either the Add Response Policy Zone Wizard or the Add DNS View wizard is displayed based on the following:
   - When you click the Add icon, the Add Response Policy Zone Wizard is displayed if you have not created additional DNS views and only have the default view.
3. If you have configured multiple DNS views, you must drill-down to the corresponding view to assign a FireEye Integrated RPZ. Click the Add icon and complete the details in the Add DNS View wizard. To create a new DNS view for your FireEye integrated RPZ, click the Add icon and complete the details in the Add DNS View wizard. For information, see Adding a DNS View. For information on modifying an existing view, see Modifying DNS Views.
4. In the Add Response Policy Zone Wizard, select Add FireEye-Integrated Response Policy Zone, click Next and specify the following:
   - **Name:** Enter the name of the FireEye integrated RPZ. It can be a combination of alphanumeric characters. You can enter up to 256 characters.
   - **DNS View:** The name of the view that you have selected is displayed by default. You can select a view from the drop-down list to associate it with the FireEye integrated RPZ.
   - **Policy Override:** Select a value from the drop-down list. You can override the policy actions that are specified in the rule level.
     - **Log Only (Disabled)** – Select this if you want to disable an RPZ rewrite using rules in the RPZ. If the response to the recursive query matches any RPZ rule, then the rule is logged, but the response will not be altered. Note that this option will not override RPZ rules in other RPZ zones, if they take precedence. Select this option to preview the rules in the syslog before they take effect.
     - **None (Given)** – Select this if you want to use the policy from the rule level.
     - **Block (No Data)** – Select this to send a response that contains no data in it.
     - **Block (No Such Domain)** – Select this if you want to receive a DNS response that indicates there is no domain. All the policy actions in an RPZ are replaced with a NXDOMAIN block.
     - **Passthru** – Select this if you want to send an actual response without modification. All the policy actions in an RPZ are replaced with the passthru action.
     - **Substitute (Domain Name)** – Select this if you want to replace all the policy actions in an FireEye integrated RPZ with the specified substitution action.
       - **Domain Name:** This appears only when you select Substitute (Domain Name) from the Policy Override list. Enter the domain name that you want the client to receive instead of the actual domain name, which is malicious or unauthorized.
       - **Comment:** Optionally, enter additional information about the FireEye integrated RPZ.
   - **Disable:** Select the check box to disable the FireEye integrated RPZ without deleting its configuration. Clear the check box to enable the FireEye integrated RPZ. For information, see Enabling and Disabling Zones.
5. Click Next to define rule mapping:
   - **Server URL:** The appliance displays the URL that you use when configuring the FireEye appliance. This URL is used to handle alerts, which is sent by the FireEye appliance. It handles alerts based on the standard authentication. The URL generated by the NIOS appliance consists of the Grid Manager IP address, network view, and DNS view of the FireEye zone. If you change the IP address, network view, zone or DNS view after you have configured a FireEye RPZ, the URL will change accordingly. Thus FireEye will not be able to send alerts to the updated URL. You must update the URL in the FireEye appliance to send alerts to the NIOS appliance. The Server URL is generated in this format:

     https://<host address>/alert/feye/<network view>/<dns view>/<zone>

   - **Rule Mapping:** You can map a FireEye alert type with an RPZ policy. Select an RPZ policy type from the drop-down list. Note that the FireEye alert type is read-only. The NIOS appliance applies corresponding RPZ policy type when the FireEye appliance sends an alert to the NIOS appliance. You can also specify a time limit for each FireEye RPZ rule depending on the FireEye alert type. NIOS displays default lifetime value for each alert type. You can change the default lifetime of the alert type. When you define a value, the value must be greater than zero. When you select Live Forever from the drop-down list, the alert type will never expire and will be stored in the database until further notice. The NIOS appliance will use the default time if you do not specify a value. You can specify the expiration time in days or weeks only. The following table lists the FireEye alerts, RPZ policy types, and the time limit for a specific FireEye alert:

<table>
<thead>
<tr>
<th>FireEye Alert Type</th>
<th>RPZ Policy Type</th>
<th>Lifetime</th>
</tr>
</thead>
</table>

Table 4.2.2 FireEye Rule Mapping

Copyright ©2019, Infoblox, Inc. All right reserved.
When you edit the lifetime of an existing alert type, NIOS deletes the alert type based on the new lifetime setting. It also updates the expiration time for the corresponding alert type. Note that there might be an impact on the performance when you delete expired FireEye RPZ rules.

- **Override rule mapping for APT events**: Select a value from the drop-down list to override rule mapping for Advanced Persistent Threats. Events that are marked as APT events by FireEye override rules that are set for other event types. The values in the drop-down list are:
  - **No Override** – Select this if you want to use the policy from the rule level and do not want to override the rule mapping settings. This value is displayed in the drop-down list, by default.
  - **Passthru** – Select this if you want the user to see the actual response without modification. All the policy actions in an RPZ are replaced with the passthru action.
  - **Block (No Such Domain)** – Select this if you want the user to receive a NXDOMAIN as the DNS response. All the policy actions in an RPZ are replaced with a NXDOMAIN block.
  - **Block (No Data)** – Select this if you want the user to receive a response that indicates that there is no data.
  - **Substitute (Domain Name)** – Select this if you want to replace all the policy actions in an RPZ with the substitution action that is specified.
  - **Substituted Domain Name**: This appears only when you select Substitute (Domain Name) from the Policy Override list either for APT events or for FireEye alerts. Enter the domain name that you want the client to receive instead of the actual domain name, which is malicious or unauthorized.

6. Click **Next** to associate the FireEye integrated RPZ with at least one primary name server:

   - Define the name servers for the FireEye integrated RPZ. A Grid name server must be recursive when primary Grid name server is used as an RPZ source. A FireEye integrated RPZ may or may not have a recursive server. For example, there could be a Grid that has only primary Grid name server for a FireEye integrated RPZ to act as an RPZ source for an external set of name servers. A FireEye integrated RPZ must have only one primary Grid name server and it can have one or more secondary Grid name servers. When you select **All Recursive Name Servers** from the list, all the recursive name servers in the Grid are added as secondary servers for the zone. For information on specifying primary or secondary name servers, see **Assigning Zone Authority to Name Servers**. For information on specifying name server groups, see **About Name Server Groups**. For information about all recursive name servers, see **Configuring RPZs for All Recursive Servers**.

7. Save the configuration and click **Next** to define extensible attributes. For information, see **About Extensible Attributes**.

8. Click **Restart** if it appears at the top of the screen.

### Configuring Rules for FireEye RPZs

You can define a list of rules based on how the DNS server determines its response to recursive queries. Based on the rules defined, responses to clients are either manipulated or forwarded without any changes. To configure rules for FireEye RPZs:

1. From the **Data Management** tab, select the **DNS** tab -> **Response Policy Zones** tab, click **DNS View** -> **Zone** and then click **Add** -> select a **Rule**.
2. The rules are classified as follows:
   - **Passthru Rule**: For information, see **Managing Passthru Rules**.
   - **Block (No Such Domain) Rule**: For information, see **Managing Block (No Such Domain) Rules**.
   - **Block (No Data) Rule**: For information, see **Managing Block (No Data) Rules**.
   - **Substitute (Domain Name) Rule**: For information, see **Managing Substitute (Domain Name) Rules**.
   - **Substitute (Record) Rule**: For information, see **Managing Substitute (Record) Rules**.
3. Complete the details in the corresponding editor.
4. Save the configuration and click **Next** to define extensible attributes. For information about extensible attributes, see **About Extensible Attributes**.

### Configuring the FireEye appliance

You must configure the FireEye appliance to send alerts to the NIOS appliance. Ensure that the following are complete before you configure the FireEye appliance:
1. Install required license on the NIOS appliance. For more information about license, see License Requirements and Admin Permissions.
2. Create a new FireEye RPZ zone. For more information, see Configuring FireEye RPZs.
3. Create FireEye admin users. For more information, see For FireEye Integrated RPZs.
4. Get the URL from the NIOS appliance and record it. You need this to configure the FireEye appliance. For more information about the Server URL, see Configuring FireEye RPZs. If you have already configured a FireEye integrated RPZ, then you can retrieve the URL through the FireEye tab of the corresponding FireEye RPZ zone. For more information about managing and retrieving the URL, see Modifying RPZs.
5. Record the usernames and passwords on the NIOS appliance. You must use these credentials when configuring FireEye alerts to enable the alerts to be received by NIOS. For more information, see Configuring the FireEye appliance to send alerts to NIOS.

**Configuring the FireEye appliance to send alerts to NIOS**

You must configure the NIOS generated URL, usernames and passwords on the FireEye appliance. FireEye appliance embeds the configured usernames and passwords in the alerts for authentication. When an alert is received, the NIOS appliance verifies the FireEye username prior to processing the alert. Note that the NIOS appliance accepts alerts sent by the FireEye appliance in JSON Normal format only. To configure a FireEye appliance:

1. Login to the FireEye appliance with your username and password.
2. In the FireEye GUI, click Settings tab and then click the Notifications tab on the left panel.
3. In the Notification Settings page, click the http link and then enter the name of the HTTP server you want to add. Click Add HTTP Server and complete the following:
   - **Name:** When you click add, the HTTP server name that you specified is listed in this column.
   - **Enabled:** Select the check box to enable alerts and notifications for the HTTP server.
   - **Server Url:** Enter the URL you received on the NIOS appliance. The alerts and notifications are sent using this URL by the FireEye appliance.
   - **Auth:** Select this check box if authentication is required for the server.
   - **Username and Password:** Enter the Username and Password of the user that you have configured for the fireeye-group on the NIOS appliance. For more information, see For FireEye Integrated RPZs.
   - **Notification:** Select a notification from the drop-down list. You can choose to include notifications for all events or only events of a selected type. The FireEye appliance will send an alert to the NIOS appliance only when selected event is encountered. When you select All Events, alerts are sent when each event is encountered by the FireEye appliance.
   - **Delivery:** Select Per Event from the drop-down list. Note that the NIOS appliance supports only Per Event selection. The FireEye appliance sends an alert each time it encounters an event.
   - **Account:** You can specify a user account name for this notification.
   - **SSL Enable:** Select this check box to enable SSL for secure transmission of alerts from the FireEye appliance to NIOS.
   - **Default Provider:** Select a default provider from the list.
   - **Message Format:** Select JSON Normal from the drop-down list. Note that the NIOS appliance supports only this message format.
4. Click Update at the bottom of the page.

**Note:** You can also click Test-Fire to test the configuration. If the configuration is successful, FireEye sends a confirmation message to the NIOS appliance and the NIOS appliance logs this message in the syslog. It generally takes a few seconds for the NIOS appliance to receive alerts. You must verify the configuration, if there is no entry in the syslog.

**Handling Alerts from the FireEye appliance**

The NIOS appliance processes each alert that it receives from the FireEye appliance. The alert contains the malware URL along with a valid FQDN. NIOS appliance can only map an alert to a RPZ rule if the FQDN is present. Once the alert is processed and properly mapped to an RPZ rule, it remains in the database until you delete it manually. When the RPZ rule is different from the existing rules, the new RPZ rule gains precedence over the existing RPZ rule in the FireEye integrated RPZ. Note that you cannot retrieve alerts that are ignored. You can get more information about the alerts, which are sent by the FireEye appliance, from the syslog. An alert will not be processed and will be ignored:

- when there are changes to the URL or if the alert does not have the malware URL or FQDN in them.
- if the zone is not found.
- if the alert is sent without any username in it or if the username does not belong to the fireeye-group.
- if a FireEye admin user is deleted. NIOS will neither authenticate the deleted user credentials nor process any future alerts with deleted user credentials.
- if the search mapping fields contain IP addresses other than FQDNs.
- if alerts contain domain names in an IPv4 or IPv6 address format.

**Logging FireEye Integrated RPZ messages**

The NIOS appliance logs FireEye events and alerts in the syslog and audit log. Each FireEye feed event is logged every time an alert is sent to NIOS by the FireEye appliance. When you create a new rule or update an existing rule, then those are also logged in the syslog. You can use messages logged in syslog to verify events that are related to communication between the FireEye and NIOS appliances. It also enables the admin to monitor alerts and verify how the alerts are processed. Details about alerts that are received and processed are also logged. Syslog messages are logged when:
• an alert is received from the FireEye appliance.
• syslog messages contain required information for reporting.
• an alert is successfully mapped to an RPZ rule. The message format is as follows:
  • <FireEye: Found an APT alert>
• the NIOS appliance cannot process alerts. For example, alert structure mismatch, unrecognizable data, etc. The messages will have the following format:
  • <FireEye: Cannot parse FQDN due to missing field"cnc-services”>
  • <FireEye: Cannot determine if it is an APT alert...>
  • <FireEye: Invalid Alert Type .....>
  • <FireEye: Couldn't find the required field...>
  • <FireEye: No mapping rule has been set for alert type.....>
• a duplicate alert is sent by the FireEye appliance for which the same RPZ rule already exists.

Note: For debugging purposes, alert messages will be displayed in the infoblox.log file.

NIOS periodically scans the syslog of a member that has RPZ license installed to generate recent hits data for the RPZ Recent Hits tab. This might cause a performance impact as CPU cycles will be used on the member. For more information about RPZ Recent Hits tab, see RPZ Recent Hits.

Configuration Examples

This section illustrates some of the examples of local and FireEye integrated RPZs.

Local RPZ Examples

Following is an example of an IP related rule. For example, execute the following command:

dig @10.35.104.19 abc.net

If the above command returns 18.58.20.1, then define an IPv4 substitute rule 18.0.0.0/8, Substitute (IPv4) 8.8.8.89.

Execute the command dig @10.35.104.19 abc.net again. You will receive the substituted address instead of the actual domain name.

Following is an example of values in CEF for the above substitution example:

2012-11-06T19:04:02+00:00 daemon (none) named[25193]: info
CEF:0|Infoblox|NIOS|6.6.0-185622|RPZ-IP|records|4|app=DNS dst=10.35.104.19
src=10.32.0.242 spt=50035 view=_default qtype=A msg="rpz IP records rewrite abc.net [A] via 8.0.0.18.rpz-ip.localrpz"

Following is an example of values in the CEF for Block (No Data) rules:

2012-11-06T19:00:01+00:00 daemon (none) named[25193]: info
CEF:0|Infoblox|NIOS|6.6.0-185622|RPZ-QNAME|NODATA|4|app=DNS dst=10.35.104.19
src=10.32.0.242 spt=50035 view=_default qtype=A msg="rpz QNAME NODATA rewrite nodata.net [A] via nodata.net.localrpz"

You can view the NIOS version, name of the view, source, and destination.

FireEye Integrated RPZ Examples

Following is an example of a syslog message when an alert gets converted to an RPZ rule:

2013-09-11T10:59:55-07:00 user (none) httpd[]: info fireeye-rpt:
'79167','infection-match','minr''eng-lab-249.inca.infoblox.com'

2013-09-11T10:59:55-07:00 user (none) httpd[]: info FireEye: Create an RPZ rule for 'd.bnksw.com' with 'SUBSTITUTE' rule in RPZ zone 'com.lock'

Note that the domain name lock.com is displayed in the reverse format.

Following is an example of a syslog message when an alert is ignored by the NIOS appliance:

2013-09-11T11:04:01-07:00 user (none) httpd[]: info fireeye-rpt:
Example of a basic RPZ Workflow

Following is an example of a basic RPZ workflow:

1. Install the RPZ license. For more information, see License Requirements and Admin Permissions.
2. Enable recursive queries for a DNS view, member, or Grid, as described in Enabling Recursion for RPZs.
3. Enable RPZ logging in the Grid DNS Properties editor to view syslog entries for RPZ queries. For more information, see Setting DNS Logging Categories.
4. Create a local RPZ. For more information, see Configuring Local RPZs.
5. Define a Substitute (PTR Record) Rule for domain name 3.3.3.5.in-addr.arpa, which is substituted with the domain name ptr1.com. For more information, see Defining Substitute Rules for PTR Records.
6. Execute the dig command to view output. The output contains the substituted domain name ptr1.com. Following is the output of an RPZ query for Substitute (PTR Record) Rule:

   $ dig @10.36.2.73 3.3.3.5.in-addr.arpa in ptr
   ; <<>> DiG 9.6.2-P2-RedHat-9.6.2-5.P2.fc12 <<>> @10.36.2.73 3.3.3.5.in-addr.arpa in ptr
   ; (1 server found)
   ;; global options: +cmd
   ;; Got answer:
   ;; ;>HEADER< opcode: QUERY, status: NOERROR, id: 7351
   ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

   ;; QUESTION SECTION:
   ; 3.3.3.5.in-addr.arpa. IN PTR

   ;; ANSWER SECTION:
   3.3.3.5.in-addr.arpa. 7200 IN PTR ptr1.com.

7. Following is the syslog entry for the query mentioned above:

   2013-09-27T02:26:46-04:00 daemon (none) named[21737]: info
   CEF:0|Infoblox|NIOS|6.9.0-218052|RPZ-QNAME|Local-Data|4|app=DNS dst=10.36.2.73
   src=10.120.20.194 spt=40518 cmd=INQ view=2 qtype=PTR msg="rpz QNAME Local-Data rewrite
   3.3.3.5.in-addr.arpa [PTR] via 3.3.3.5.in-addr.arpa.local1.com"

For more information about syslog, see Viewing RPZ in the Syslog.

Mitigating Cyber Threats using TAXII

To mitigate the increasingly complex cyber attacks, you can enable the appliance to run a TAXII (Trusted Automated eXchange of Indicator Information) service to receive information on real-time threat incidents. The information in each threat incident is represented using the STIX (Structured Threat Information eXpression) language format. STIX is a standard language used to describe structured cyber threat information, which is shared between different TAXII clients.

When you run the TAXII service on a Grid member, the appliance acts as a TAXII server that receives TAXII messages (for one or more specified STIX collection) from TAXII clients. The TAXII message typically contains a list of IP addresses (both IPv4 and IPv6) and domains. The member then communicates with the Grid Master and sends a request to create an RPZ rule on the specified RPZ based on the TAXII messages it receives. The RPZ rule created on NIOS is available in the Response Policy Zones tab, as shown in Figure 42.4.

Note: Once you start the TAXII server, the inbox for the configured collections is available at https://<member address>/services/inbox and the TAXII discovery service is available at https://<member address>/services/discovery, where <member address> is the MGMT or LAN IP address (IPv4 or IPv6 address of the port that is configured).

For more information about TAXII and STIX, refer to the following:

https://taxii.mitre.org/
Supported Appliances for TAXII Service

You can run the TAXII service on the following Infoblox appliance models: IB-1410, IB-1415, IB-1420, IB-1425, IB-VM-1410, IB-VM-1415, IB-VM-1420, IB-VM-1425, TE-810, TE-815, TE-2210, TE-2215, TE-2220, TE-2225, IB-VM-4010, IB-4030, IB-4030-10GE, IB-VM-2220, IB-VM-2225, PT-1400, PT-1405, PT-2200, PT-2205, PT-2205-10GE, PT-4000, and PT-4000-10GE.

Licensing Requirements and Permissions

To enable the TAXII service, you must install the **Security Ecosystem** license on any Grid member. You must also install an **RPZ** license on any Grid member in the Grid in order to create RPZ rules based on the TAXII messages. To allow a group to access the TAXII service, you can enable the group to authenticate with the TAXII server.

To enable a group to access the TAXII server:

1. From the **Administration** tab, select the **Administrators** tab -> **Groups** tab, and then click the Add icon.
2. In the **Add Admin Group wizard**, click the **Roles** tab and then complete the following in the **Allowed Interfaces** section:
   - **TAXII**: Select this check box to enable a group to authenticate with the TAXII server.
3. Save the configuration.

Mapping RPZs with TAXII Collections

NIOS supports arbitrary set of RPZ rules mapped to the corresponding TAXII collection. To map an RPZ with a TAXII collection:

1. From the **Grid** tab, select the **Grid Manager** tab -> **Services** tab.
2. In the **Services** tab, select the **TAXII_member** check box, and then click **Edit** -> **Member TAXII Properties** from the Toolbar.
3. In the **Member TAXII Properties** editor, complete the following:
   - **Response Policy Zone**: Click the Add icon and click **Select RPZ** to select an RPZ. When there are multiple zones, Grid Manager displays the **Zone Selector** dialog box from which you can select one.
   - **Collection**: Enter the name of the TAXII collection that will be mapped to the RPZ. Note that you can only use valid URI characters as collection names. You cannot use special characters or spaces.
   - **Add**: Click the Add icon to add the RPZ and collection name to the table.
   - **Save and Close**: Click this to save the configuration and close the editor.

You can do the following in this tab:

- To edit an entry in the list, click the check box beside an RPZ, and then click the Edit icon.
- To delete an entry in the list, select the check box beside an RPZ, and then click the Delete icon.

![Figure 42.3 Mapping RPZs with TAXII Collection](image)
Figure 42.4 RPZ Rules created for the Mapped RPZ and Collection

Starting and Stopping the TAXII Service

To start the TAXII service:
1. From the Grid tab, select the Services tab -> TAXII_member check box and then click the Start icon from the vertical Toolbar.

To stop the TAXII service:
1. From the Grid tab, select the Services tab -> TAXII_member check box and then click the Stop icon from the vertical Toolbar.

Extensible Attributes for TAXII Service

You can define extensible attributes that are specific to the TAXII service, as described in Extensible attributes for TAXII service. When you define TAXII specific extensible attributes, the RPZ rules created will have these attributes and their corresponding values (received in the TAXII messages) added automatically.

For information about how to configure extensible attributes, see About Extensible Attributes.

Table 42.3 Extensible attributes for TAXII service

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAXII_collection</td>
<td>String</td>
<td>The name of the TAXII collection the TAXII client delivered the message to.</td>
</tr>
<tr>
<td>TAXII_source</td>
<td>String</td>
<td>The IP address of the TAXII client that sent the TAXII message.</td>
</tr>
<tr>
<td>TAXII_member</td>
<td>String</td>
<td>The TAXII Grid member that receives TAXII message resulting in the creation of the RPZ rule.</td>
</tr>
<tr>
<td>TAXII_timestamp</td>
<td>Date/Integer</td>
<td>The timestamp when the TAXII message was received.</td>
</tr>
<tr>
<td>TAXII_user</td>
<td>String</td>
<td>The login name of the user the TAXII client connected as to the TAXII server on the member that received the message.</td>
</tr>
</tbody>
</table>

Monitoring TAXII Server

You can monitor the status of the TAXII server, as described in Monitoring Grid Services. If there are any invalid TAXII messages, the appliance makes a syslog entry. For information, see Viewing RPZ in the Syslog. The appliance also sends an SNMP trap and an email notification, if configured. For information about setting SNMP and email notification, see Setting SNMP and Email Notifications.

Managing RPZs

You can manage RPZs that you defined earlier and modify their information. You can do the following:
Viewing RPZs

You can view the list of RPZs, local, feed, or FireEye integrated RPZs, which are currently listed in the Grid. To view RPZs:

1. From the Data Management tab -> DNS tab -> Response Policy Zones tab.
2. Grid Manager displays the following:
   - **Order**: Displays the order of RPZs. The order value is empty if you do not assign a primary name server when configuring a local RPZ, or if the local RPZ or the service is disabled.
   - **Name**: Displays the name of the RPZs. Click the RPZ link to view the following details:
     - **Name or Address**: Displays the domain name or the IP address.
     - **Policy**: Defines the policy defined for the corresponding domain name or IP address.
     - **Data**: Displays the target data of the rule.
     - **Comment**: Displays the comment specified when an RPZ is defined.
     - **Disabled**: Displays Yes if the RPZ rule is disabled.
     - **Site**: Displays extensible attributes that are associated with the domain name or IP address.
   - **Type**: Displays the type of RPZs, that is, **Local**, **Feed**, or **FireEye**.
   - **Primary Name Server**: Displays the primary name server that is associated with an RPZ.
   - **Last Updated**: Displays the last updated time. For RPZ feed, it indicates if the RPZ feed has stalled and when the last zone transfer happened. For a local and FireEye integrated RPZ, it indicates the last time the zone or data was modified.
   - **The last updated time is empty, if:**
     - A local RPZ is not associated with a primary Grid name server.
     - A zone, either a local RPZ or an RPZ feed, is not enabled.
     - An inbound zone transfer has not occurred for an RPZ feed.
     - Member's DNS service is disabled.
   - **Comment**: Displays the comment recorded when creating the zone. You can double-click on a row to edit the comment. Click Save after modification.
   - **Disabled**: Displays Yes if the RPZ is disabled. Otherwise, this field displays No.
   - **Locked**: Displays Yes when a zone is locked by an admin, and displays No when the zone is unlocked.
   - **Site**: Displays the values that were entered for this pre-defined attribute. You can double-click on a row to edit the Site. Click Save after modification.

You can also do the following:

- Use QuickFilter and the Goto function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Goto field and select the object from the possible matches. Select a value from the drop-down list to filter the RPZs.
  - **None**: Select this to display all the RPZs that you have configured.
  - **All Local Response Policy Zones**: Select this to list only the local RPZs.
  - **All Feed Response Policy Zones**: Select this to list only the RPZ feeds.
  - **All FireEye Response Policy Zones**: Select this to list only the FireEye RPZs.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- You can create a bookmark for the RPZs. For information, see Using Bookmarks.
- You can modify some of the data in the table. Double-click a row of data, and either edit the data in the field or select an item from a drop-down list. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
- To export the list of RPZs to a .csv file, click the Export icon. For information on the export options, see About CSV Import.
- Click the Print icon to print the list of RPZs. For more information, see Printing from Grid Manager.

Modifying RPZs

You can modify the name servers or name server groups, update policy override details and permissions, or edit extensible attributes that are associated with an RPZ. Note that if you have configured a client IP address or network rule for a local RPZ, you cannot associate an Infoblox-4030 appliance as a Grid primary or a Grid secondary name server with that local RPZ.

To modify RPZs:

1. From the Data Management tab -> DNS tab -> Response Policy Zones tab -> Response Policy Zone check box and then click the Edit icon.

Copyright ©2019, Infoblox, Inc. All right reserved.
2. The RPZ editor provides the following tabs from which you can modify data:
   - In the **General** tab, you can change the information you previously entered through the wizard, as described in Configuring Local RPZs. For FireEye integrated RPZs, you can update the policy type, comments, enable or disable, or lock the zone. For more information, see Configuring FireEye RPZs.
   - For a FireEye integrated RPZ, the **FireEye** tab is displayed. This tab is displayed only after you install the FireEye license. You can modify or override the rule mapping for FireEye alerts or APT events. For more information, see Configuring FireEye RPZs.
   - You can also enter or edit information in the **Name Servers**, Extensible Attributes, **Settings** and **Permissions** tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.

3. Save the configuration and click **Restart** if it appears at the top of the screen.

Reordering RPZs

You can change the order of RPZs, local feeds, or FireEye integrated RPZs, in each view. When you add a new local RPZ, it is added to the top of the zone list and an RPZ feed is automatically added to the bottom of the zone list. You can change the order of each through the re-ordering process.

The policy override works based on zone ordering. The zone at top has the highest priority and it overrides the lower priority zone. To override an RPZ feed with a local RPZ, place the local feed at the top before an RPZ feed. You cannot reorder zones, if they are disabled or do not have any primary name server assigned.

To reorder RPZs:

1. From the **Data Management** tab, select the **DNS tab** -> **Response Policy Zones** tab, click **Order Response Policy Zones** from the **Toobar**.
2. The following are displayed in the **Order Response Policy Zones** wizard:
   - **Ordering**: Use the up and down arrows to move the RPZ to the desired order.
   - **Response Policy Zone**: Displays all the RPZs.
   - **Priority**: Displays the order of RPZs.
3. Click **OK** to save the changes.

Locking and Unlocking RPZs

You can lock an RPZ so you can make changes to it and prevent others from making conflicting changes. When you lock an RPZ, Grid Manager displays LOCKED beside the RPZ. When other administrators try to make changes to a locked RPZ, the system displays a warning message that the RPZ is locked and the name of the admin who locked the RPZ.

Only a superuser or the administrator who locked the RPZ can unlock it. RPZ locks do not expire; you must manually unlock a locked RPZ. To lock or unlock RPZs:

1. From the **Data Management** tab, select the **DNS tab** -> **Response Policy Zones** tab, select the **Response Policy Zone** -> **Ruleset**.
2. You can do the following:
   - **To Lock**: Click the **Lock** icon to lock the zone.
   - **To Unlock**: Click the **Unlock** icon to unlock the zone.

Deleting RPZs

You can delete RPZs or schedule them for deletion for a later date. The NIOS appliance moves the deleted RPZs to the Recycle Bin, if enabled. When you restore the zone from the Recycle Bin, it will be restored to the bottom of the zone list.

To delete RPZs:

1. From the **Data Management** tab, select the **DNS tab** -> **Response Policy Zones** tab, select **Response Policy Zone** -> **Ruleset**.
2. To delete an RPZ immediately, click the **Delete** icon, and then click **Yes** to confirm the delete request. To schedule the deletion, click **Schedule Deletion** and in the **Schedule Change** panel, enter a date, time, and time zone. For information, see **Scheduling Deletions**.

Grid Manager moves the RPZ to the Recycle Bin, from which you can restore or permanently delete it.

Managing RPZ Rules

You can manage local RPZ, including FireEye integrated RPZ rules that you defined earlier and modify their information. You can do the following:

- View RPZ rules, as described in **Viewing RPZ Rules**.
- Modify RPZ rules, as described in **Modifying RPZ Rules**.

**Note:** You cannot modify the rules of an RPZ feed. However, you can override the entire ruleset or each rule using local RPZs.

- Delete RPZ rules, as described in **Deleting RPZ Rules**.
- Copy RPZ rules, as described in **Copying RPZ Rules**.
- Import RPZ rules, as described in **Importing RPZ Rules**.
- Disable NSDNAME and NSIP rules for RPZ zones, as described in **Disabling NSDNAME and NSIP rules for RPZ zones**.
Viewing RPZ Rules

You can view and edit the rules that are defined for each local RPZ, including FireEye integrated RPZs. To view RPZ rules:

1. From the Data Management tab -> DNS tab -> Response Policy Zones tab -> click the RPZ link.
2. You can view the following:
   - **Name or Address**: Displays the domain name or the IP address on which the rule is defined.
   - **Policy**: Displays the rule applied on the domain name or the IP address.
   - **Data**: Displays the target data of the rule.
   - **Comment**: Displays the comment specified when the rule is defined.
   - **Disabled**: Displays Yes if the RPZ rule is disabled. Otherwise, this field displays No.
   - **Site**: Displays an extensible attribute, Site.
   - **Expiration**: Displays the expiration time for the corresponding FireEye integrated RPZ rule. Note that NIOS updates the expiration time when you change the lifetime of the FireEye integrated RPZ rule, or if the last updated time of the rule changes, or if the alert type that generates the rule changes. This time is estimated based on the following:
     
     \[
     \text{Expiration Time} = \text{Lifetime of an alert type} + \text{Last updated time of the rule}
     \]
     
     NIOS runs a scheduler every 10 minutes to identify FireEye integrated RPZ rules whose expiration time is less than the current time. If there are rules whose expiration time is less than the current time, then such rules will be deleted. NIOS logs all deletion activities in the syslog. You can view the syslog to verify expired rules. For more information, see Viewing RPZ in the Syslog.
   - **FireEye Alert Type**: Displays the type of FireEye alert.
   - **Last Updated**: Displays the time when the RPZ rule was last updated.

**Note**: The columns, **Expiration**, **FireEye Alert Type**, and **Last Updated**, are displayed only for FireEye integrated RPZ rules. These columns are not displayed for non-FireEye RPZ rules.

You can also do the following:

- Use **Quick Filter** and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria. For information, see Using Quick Filters.
- Modify some of the data in the table. Double click a row of data, and either edit the data in the field or select an item from a drop-down list. You can edit **Comments** and **Extensible Attributes**. Note that some fields are read-only. For more information about this feature, see Modifying Data in Tables.
- To export the list of RPZ rules to a .csv file, click the Export icon. For information on the export options, see About CSV Import.
- Click the Print icon to print the list of RPZ rules. For more information, see Printing from Grid Manager.

Modifying RPZ Rules

You can modify the name of a local or FireEye integrated RPZ rule, IP address, network address, substituted name, and the comment recorded for the corresponding rule. You can also update the TTL settings or the extensible attributes that are associated with an RPZ rule.

To modify RPZ rules:

1. From the Data Management tab -> DNS tab -> Response Policy Zones tab -> click the RPZ link -> Name or Address check box, and then click the Edit icon.
2. The RPZ rules editor provides the following tabs from which you can modify data:
   - In the **General** tab, you can change the information you previously entered through the wizard. For more information, see Configuring Rules for RPZs.
   - You can also enter or edit information in the **TTL and Extensible Attributes** tabs. For information about TTL settings, see About Time To Live Settings. For information about extensible attributes, see About Extensible Attributes.
3. Save the configuration.

Deleting RPZ Rules

You can delete local RPZ rules, including FireEye integrated RPZ rules, or schedule them for deletion for a later date. When you remove an RPZ rule, the NIOS appliance moves it to the Recycle Bin, if enabled.

To delete RPZ rules:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab -> Response Policy Zone -> Ruleset.
2. To delete an RPZ rule immediately, click the Delete icon, and then click Yes to confirm the delete request. To schedule the deletion, click **Schedule Deletion** and in the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Deletions.

Grid Manager moves the RPZ rule to the Recycle Bin, from which you can restore or permanently delete it.
Copying RPZ Rules

You can copy rules from one local RPZ to another local RPZ or from one FireEye integrated RPZ to another FireEye RPZ. You can also copy rules from a local RPZ to a FireEye integrated RPZ or vice-versa. Different views of the same RPZ may have a number of rules in common. If this is the case, you can copy rules between views and zones.

To copy RPZs between DNS zones and views:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab, click Copy Rules from the Toolbar.
2. In the Copy Rules dialog box, Grid Manager displays the last selected zone or the zone from which you are copying rules in the Source field. The following fields are displayed:
   - Source: Grid Manager displays the last selected zone or the zone from which you are copying rules. It also displays the associated DNS view.
   - Destination: Click Select Zone to select the destination zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box from which you can select one. After you select the zone, Grid Manager displays the associated DNS view.
   - Copy All Rules: Select this option to copy all the rules.
   - Copy Specific Rules: Select this option to copy specific rules only. Select a rule from the Available column and click the right arrow to move it to the Selected column.
   - Copy Options: Select one of the following:
     - Delete all rules in the destination before copying the rules: Select to delete all rules in the destination zone before the records are copied.
     - Overwrite existing rules: Select to overwrite existing rules that have the same domain name owners as the rules being copied.
3. Click Copy & Close.

Importing RPZ Rules

You can import rules from an RPZ zone to a local zone. To import, you must enable zone transfer on the external server. The rules of the existing zone are overwritten when you import rules from an external server.

To import RPZ rules:

1. From the Data Management tab, select the DNS tab -> Response Policy Zones tab -> click the RPZ link in the Name column -> Rules, click Import Zone from the Toolbar.
2. In the Import Zone dialog box, the following fields are displayed:
   - Zone: The RPZ that you have selected is displayed.
   - DNS View: The DNS view that you have selected is displayed.
   - Address: Enter the address of the external server from where you want to import rules.
3. Click Import.

Disabling NSDNAME and NSIP rules for RPZ zones

NSDNAME and NSIP rules are enabled for RPZ zones by default. You can disable or enable NSDNAME and NSIP rules to control the validation of NS records and glue records received by upstream DNS servers. When you enable RPZ on internal DNS servers and if there are forward-mapping zones that are not reachable from external networks, NSDNAME and NSIP validation is not necessary. In this case, you can disable NSDNAME and NSIP rules to reduce delays in responses. When you disable these rules for RPZ zones, the appliance bypasses NSDNAME and NSIP validation for the queries and it significantly improves the performance. Note that this setting disables both NSDNAME and NSIP rules at the same time for both internal and external RPZ zones. This setting only affects the lookup process but the zone data remains unchanged. NSDNAME and NSIP records will still be available in RPZ zones during zone transfers (AXFR and IXFR). If you disable NSDNAME and NSIP rules for RPZ zones at the Grid level, all members inherit this setting. You can override this setting for each member.

Note: Disabling NSDNAME and NSIP rules for RPZ zones on members which may send recursive queries to external servers, results in reduced security. Accordingly, it is not recommended to disable these rules for RPZ zones on members that respond with data from external servers.

To disable NSDNAME and NSIP rules for RPZ zones:

1. Grid: From the Data Management tab, select the DNS tab, expand the Toolbar and click Grid DNS Properties. Member: From the Data Management tab, select the DNS tab, click the Members tab -> member check box -> Edit icon.
2. In the Grid DNS Properties or Member DNS Properties editor, click the General tab -> Advanced tab and complete the following:
   - Disable NSDNAME and NSIP rules for RPZ zones: This check box is deselected and NSDNAME and NSIP rules are enabled for RPZ zones by default. Select this check box to disable NSDNAME and NSIP rules for all RPZ zones. To override the value inherited from the Grid, click Override. To retain the same value as the Grid, click Inherit.
3. Save the configuration and click Restart if it appears at the top of the screen.

Configuring Prefix Length Limit for RPZ-IP Triggers
To avoid the possibility of DNS outage resulting from errors in the RPZ rules received from external sources by the RPZ feed or due to errors in the RPZ rules added to local RPZ, Infoblox provides an option to set the prefix length limit for RPZ-IP triggers. This enables the appliance to ignore RPZ-IP rules with prefix lengths that are less than the configured minimum prefix length, and to enforce only those RPZ-IP rules whose prefix lengths are equal to or greater than the configured minimum prefix length, thus accepting legitimate queries instead of dropping all queries. For example, if you configure 24 as the minimum IPv4 prefix length, the Grid enforces only those RPZ-IP rules with prefix length equal to or greater than 24 and the RPZ-IP rules with prefix lengths less than 24 are not enforced on queries that originate from external sources. You can configure the prefix length limit for IPv4 and IPv6 prefixes at the Grid level and override it for a member, DNS view, or RPZ zone. The appliance logs a warning message in the syslog when RPZ-IP rules with prefix length less than the configured minimum prefix length are added to the local RPZ and, when an RPZ feed receives RPZ-IP rules with prefix length less than the configured prefix length from external sources.

To configure the prefix length limit for RPZ-IP triggers:

1. Grid: From the Data Management tab, select the DNS tab, and then select Grid DNS Properties from the Toolbar.
   Member: From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon.
   DNS View: From the Data Management tab, select the DNS tab and click the Zones tab -> dns_view check box -> Edit icon.
   RPZ Zone: From the Data Management tab, select the DNS tab -> Response Policy Zones tab -> Response policy zone check box -> Edit icon.
2. In the editor, click Toggle Advanced Mode, and then select the Security tab.
3. Complete the following in the Response Policy Zones section of the Security tab:
   - Ignore RPZ-IP triggers with too small prefix lengths: Select this check box to set the prefix length limit for RPZ-IP triggers and enable the appliance to ignore the RPZ-IP rules with prefix lengths that are less than the specified prefix length limit. This check box is deselected by default.
     - Minimum IPv4 Prefix Length: Enter the minimum prefix length for IPv4 prefixes. You can specify a value between 1 to 31. The default value is 29.
     - Minimum IPv6 Prefix Length: Enter the minimum prefix length for IPv6 prefixes. You can specify a value between 1 to 127. The default value is 112.
4. Save the configuration and click Restart if it appears at the top of the screen.

Configuring Thresholds for RPZ Hit Rate

When the RPZ hit rate, which is the ratio of the number of queries that result in modifying the genuine response due to RPZ rules to the total number of incoming queries is high, it is unexpected and might warrant your attention. Note that the queries that hit passthru RPZ rules are not considered for the RPZ hit rate. You can configure thresholds for RPZ hit rate, above which the appliance makes a syslog entry and sends alerts as SNMP traps and email notifications. Note that you must enable notifications in order for the appliance to send SNMP traps and email notifications. For information about setting the SNMP trap and email notifications, see Setting SNMP and Email Notifications.

Note that the appliance calculates the RPZ hit rate globally for all DNS views and sometimes the RPZ hit rate might be misleading. For example, if there are multiple DNS views with or without RPZ rules, there is a possibility that some DNS views might receive a substantial number of normal queries, obscuring the possible high RPZ hit rate in the other DNS views. Also, when the DNS server is configured for both authoritative and recursive queries, it is possible that the authoritative zones receive a substantial number of queries for which RPZ rules are not considered. It might make the resulting RPZ hit rate normal even if there is an excessive number of hit for recursive queries.

To configure the thresholds for RPZ hit rate:

1. Grid: From the Grid tab, select the Grid Manager tab, and then select Grid Properties -> Edit from the Toolbar. Member: From the Grid tab, select the Grid Manager -> Members tab -> member, and then click the Edit icon.
2. In the Grid Properties or Grid Member Properties editor, click Toggle Advanced Mode, and then select the SNMP Threshold tab.
3. Complete the following in the Response Policy Zones Hit Rate Configuration section of the SNMP Threshold tab.
   - RPZ Hit Rate: Click Override to override the inherited settings, and specify the following:
     - Trigger %: Enter the Trigger value between 0 and 100. If the RPZ hit rate equals the Trigger value, the appliance logs a syslog entry and — if configured to do so — sends an SNMP trap and an email notification. The default Trigger value is 10%.
     - Reset %: Enter the Reset value between 0 and 100. If the RPZ hit rate equals the Reset value, the appliance logs a syslog entry and — if configured to do so — sends an SNMP trap and an email notification, to notify that the RPZ hit rate has gone back to an acceptable level. The default Reset value is 2%.
     - Interval: Enter the time interval that determines when the appliance starts calculating the RPZ hit rate. You can enter a value between 1 and 86400. The default value is 10 seconds. At the end of each interval, if the number of incoming queries equals or exceeds the Minimum query value, the appliance calculates the RPZ hit rate and if the RPZ hit rate exceeds the Trigger value, the appliance sends notifications and continues to send notifications at the end of subsequent intervals, until the RPZ hit rate equals the Reset value. Note that the appliance calculates the RPZ hit rate at the end of each Interval or when the number of incoming queries reach the Maximum query value, whichever comes sooner.
     - Minimum query: Specify the minimum number of queries received between the RPZ hit rate checks. The default value is 1000. The appliance calculates the RPZ hit rate when the number of incoming queries equals or exceeds the Minimum query value at the end of the Interval. If the total number of incoming queries is less than the Minimum query value, the appliance skips the RPZ hit rate check and the query count continues to cumulate into subsequent intervals until the Minimum query is met.
     - Maximum query: Specify the maximum number of queries received between the RPZ hit rate checks. The default value is 100000. When the number of incoming queries equals or exceeds this value, the appliance calculates the RPZ hit rate and does not wait for the expiration of the Interval.
4. Save the configuration and click **Restart** if it appears at the top of the screen.

**Verifying RPZ Configuration**

After you have set up and configured RPZs and RPZ rules, you can verify whether the RPZ zone transfers are functioning properly by doing the following:

- View the RPZ syslog messages, as described in [Viewing RPZ in the Syslog](#).
- Verify the last RPZ updates, as described in [Viewing the Last Updated RPZs](#).

The appliance also makes a syslog entry, when an RPZ zone refresh succeeds or fails and also sends an SNMP trap and an email notification, if configured. For information about setting SNMP and email notification, see [Setting SNMP and Email Notifications](#).

**Viewing RPZ in the Syslog**

To receive RPZ information in the syslog, make sure that you enable the RPZ option in the Logging tab of the Grid DNS Properties editor. For information about configuring logging properties, see [Setting DNS Logging Categories](#). Once the RPZ option is enabled, the appliance logs RPZ threats in CEF (Common Event Format) in the syslog. You can click the Action icon to view the RPZ threat details in the RPZ Threat Details viewer. For information about how to configure the syslog server, see [Using a Syslog Server](#).

Following is a sample RPZ threat message:

```
2014-09-15T07:14:47-07:00 daemon info rpz:
CEF:0|Infoblox|NIOS|6.12.0-252689|RPZ-QNAME |PASSTHRU|7|app=DNS dst=172.31.1.156
src=10.120.20.69 spt=39503 view_default qtype=A msg="rpz QNAME PASSTHRU rewrite
passthru.com [ANY] via passthru.com.rpz_1.com
```

Each log message contains the following information:

- The timestamp when the event happened in `yyyy-mm-ddThh:mm:ss-00:00` format.
- `Infoblox|NIOS` indicates the Infoblox product, and `x.x.x` represents the NIOS version.
- The string following the NIOS version is a hard-coded constant. In this example, it is `RPZ-QNAME`.
- The hard-coded constant is followed by mitigation action. In this example, it is `PASSTHRU`.
- The number following the mitigation action is the threat severity level. The following numbers indicate the severity levels:
  - 8 = Critical
  - 7 = Major
  - 6 = Warning
  - 4 = Informational
- `dst`: Destination IP address.
- `src`: Source IP address.
- `spt`: Source port.
- `view`: DNS view.
- `qtype`: Query type.
- `msg`: RPZ rule.

The syslog messages are optionally tagged according to the logging category configured in the external syslog servers. For more information, see [Syslog Message Prefixes](#).

To verify RPZ zone transfers:

1. Go to the **Administration** tab -> **Logs** tab -> **Syslog** tab.
2. Select **RPZ Incident Logs** from the **Quick Filter** drop-down list.
3. Review the syslog for zone transfer confirmation, as shown in **Figure 42.5**.

*Figure 42.5 The Syslog Viewer*
### Viewing the Last Updated RPZs

To view the last updated RPZs:

1. Go to the **Data Management** tab -> **DNS** tab -> **Response Policy Zones** tab.
2. Review the **Last Updated** column and confirm the time when an RPZ was last updated, as shown in **Figure 42.6**.

**Note:** It may take up to 10 minutes before the updated information is displayed.

### Chapter 44 Cisco ISE Integration

This chapter describes how to integrate Cisco ISE (Identity Services Engine) into the NIOS appliance to enhance identity management across devices and applications that are connected to your network routers and switches. It provides guidelines about how to subscribe and publish contextual data, and add notification rules. By integrating Cisco ISE, you can gain greater visibility in user and device information, thereby enhances security across your network resources. It includes the following sections:

- Integrating Cisco ISE into NIOS
- NIOS Licensing Requirements
- Administrative Permissions
- Prerequisites
- Generating Certificates
Integrating Cisco ISE into NIOS

With the rapid growth of BYOD (Bring Your Own Device) trend, the complexity of securing network resources has become more challenging. To ensure data privacy and security of all network resources against threats, Infoblox introduces the **Ecosystem** feature that allows you to expand the visibility of networks, users, and devices. Using this feature improves overall IT operations by sharing information between network and security teams.

Integrating Cisco ISE server into NIOS enables NIOS and Cisco ISE to exchange valuable network, user, device, and security-event information, enriching both Infoblox DDI and Cisco ISE data. Cisco ISE is a centralized security solution (Network Access Control) that automates and enforces context-aware security access to network resources. NIOS supports the integration of Cisco ISE versions 1.3, 1.4, and 2.0. This feature ensures that only the authorized users from legitimate devices get access to the services they need.

**Note:** Cisco ISE does not support IPv6 addresses.

When you configure a Cisco ISE, you can do the following:

- **Subscribe to contextual data:** NIOS acts as a client to the Cisco ISE and collects information about the subscribed data types. You can configure extensible attributes without restricting them to specific object types, and then map these extensible attributes to Cisco ISE data to collect additional information. You can view subscribed information collected from the Cisco ISE in the appropriate tabs (IPAM, IP Map panel, and Network Users) of the Infoblox GUI. For information about how to subscribe to contextual data, see **Configuring Cisco ISE on NIOS**. You can also monitor subscription data using the **Subscription** report. For information, see **Subscription Data**.

- **Publish contextual data** - You can publish contextual data from NIOS to specific Cisco ISE based on the conditions and criteria specified in the notification rules. To publish RPZ and threat protection notifications, you must first set up an external syslog server, as described in **Specifying Syslog Server for Notifications**. For information about notification rules, see **Configuring Notification Rules**. You can monitor published data using the **Publish Data** report through the Reporting and Analytics feature. For information about this report, see **Publish Data**.

NIOS Licensing Requirements

You must install the **Network Insight** license to configure Cisco ISE. You might need the following licenses to configure notification rules for RPZ and threat protection event types:

**Table 44.1 Required Licenses**

<table>
<thead>
<tr>
<th>License</th>
<th>Event Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPZ</td>
<td>DNS RPZ</td>
</tr>
<tr>
<td>Threat Protection</td>
<td>Security ADP</td>
</tr>
<tr>
<td>DNS, DHCP, and MSGMGT</td>
<td>IPAM</td>
</tr>
<tr>
<td>DNS and DHCP</td>
<td>DHCP Lease</td>
</tr>
</tbody>
</table>

For information about how to install licenses, see **Managing Licenses**.

Administrative Permissions

By default, only superusers can add, edit, and delete Cisco ISEs. Limited-access admin groups can access Cisco ISEs only if their administrative permissions are defined. For information about administrative permissions, see **About Administrative Permissions**.

Prerequisites

Do the following before you begin using this feature on NIOS:

- Cisco ISE uses SSL certificates as the method of authentication. You must upload the client certificate and client key when configuring the Cisco ISE server. You can include both client certificate and key in a single file and then upload. For information, see **Generating Certificates**.
Note: Make sure to use the host name of the Grid member that is selected as the subscribing member. The host name of the subscribing member must match with the Common Name that you mention while generating the certificate.

- For the bulk download certificate, download the server certificate from the monitoring node. If the admin node and monitoring node are on one node, then download the certificate from the admin node. Log into Cisco ISE and download the default self-signed server certificate (Administration -> System -> Certificates -> Export).
- For the CA certificate, download the CA certificate from the admin node or the self-signed certificate (Administration -> System -> Certificates -> Export).
- Register NIOS as a client on the Cisco ISE. You must enable the Auto-Registration option on the Cisco ISE: From the Administration menu -> click pxGrid Services, and then click Enable Auto-Registration. For more information, refer to Cisco ISE documentation. When you register NIOS successfully, you can view infoblox_client_subscribe_xxxx and infoblox_client_publish_xxxx, where xxxx is a number generated based on the IP of the subscribing member on the Cisco ISE. If auto-registration is not enabled, approve the pxGrid client after registration. If you change the certificates, Cisco ISE may not register the client successfully. In this case, delete the related pxGrid client from the Cisco ISE server, which is automatically created again.
- Enable the Identity Mapping feature on the NIOS appliance:
  a. From the Grid tab, select the Grid Manager tab -> Grid Properties -> Edit from the Toolbar.
  b. In the Grid Properties Editor, select the General tab -> Advanced tab, select the Enable network users feature check box.
- To publish data:
  - To publish dynamic data, such as DHCP lease and IPAM information, make sure that you approve Infoblox_DHCP and Infoblox_IPAM on the Cisco ISE, and then configure notification rules as described in Configuring Notification Rules.
  - To publish RPZ and threat protection notifications to the Cisco ISE server, you must first set up an external syslog server and then configure notification rules, as follows:
    a. Configure an external syslog server that listens on port 2000, as described in Specifying Syslog Server for Notifications.
    b. Set up notification rules, as described in Configuring Notification Rules.

Note: Refer to Cisco ISE documentation for information about how to perform auto-registration, creating authorized groups, and approving dynamic topics.

Generating Certificates

To generate a self-signed key and certificate:

1. openssl genrsa -out self1.key 4096
2. openssl req -new -key self1.key -out self1.csr
3. openssl req -x509 -days 365 -key self1.key -in self1.csr -out self1.cer

For CSR request:

Country Name (2 letter code) [XX]: <Country Name>, for example: US
State or Province Name (full name) []: <State Name>, for example: CA
Locality Name (eg, city) [Default City]: <City Name>, for example: SC
Organization Name (eg, company) [Default Company Ltd]: <Company Name>, for example Infoblox
Organizational Unit Name (eg, section) []: <Organization Name>, for example: QA
Common Name (eg, your name or your server's hostname) []: <host name of the subscribing member>
Email Address []:

Enter the following 'extra' attributes to be sent with your certificate request:

A challenge password []:

Import the certificate generated in step 3 to Cisco ISE's trusted store. Select the Trust for authentication within ISE check box.

Export the self-signed ISE certificate of the ISE server (under System -> Certificates). Make sure to select the pxGrid: Use certificate for the pxGrid Controller check box before exporting it.

You can call this as isemnt.cert

Wait for ISE services to restart. It may take a few minutes.

Configuring Cisco ISE on NIOS
You can configure Cisco ISE servers 1.3, 1.4 and 2.0 on the NIOS appliance. You can subscribe for identity information that you wish to collect from the Cisco ISE, such as user name, domain name, VLAN, session state, SSID, endpoint profile, and security group. You can also add extensible attributes without restricting it to specific object types, and map these extensible attributes with the Cisco ISE field types to collect additional information. Note that you can subscribe to only one Cisco ISE per member and each member can subscribe to only one Cisco ISE. You can publish ADP and RPZ notifications, DHCP and IPAM information from NIOS to Cisco ISEs based on the notification rules that you have configured. Note that you can publish DHCP lease and IPAM information only to Cisco ISE 2.0. You can view the subscribed information from the IPAM tab and the IP Map panel. Make sure that you synchronize time between the managing member and Cisco ISE.

**Configuring Cisco ISE Servers**

To configure a Cisco ISE server:

1. From the **Grid** tab, select the **Ecosystem** tab, and then click the **Add Cisco ISE** from the Toolbar.
   - From the **Grid** tab, select the **Ecosystem** tab, and then click the **Add Cisco ISE** from the Toolbar.
2. In the **Add Cisco ISE** wizard, complete the following.
   - **Server Address:** Enter the IP address of the Cisco ISE.
   - **Version:** Select the version of the Cisco ISE.
   - **Subscribing Member:** Click Select to select a Grid member that you want to subscribe as the client on the Cisco ISE. In the **Member Selector** dialog box, select a Grid member from the list. This member interacts with the Cisco ISE to obtain contextual information for the subscribed data types.
   - **Network View:** This appears only when you have multiple network views. From the drop-down list, select the network view in which you want to create the network.
   - **Client Certificate:** Click Select to upload the client certificate. In the **Upload** dialog box, click Select to navigate to the certificate, and then click **Upload**.
   - **Bulk Download Certificate:** Click Select to download the server certificate from the monitoring node or self-signed certificate.
   - **Manage Certificates:** Click **CA Certificates** to upload the self-signed certificate or CA certificate. In the **CA Certificates** dialog box, click the **Add** icon, and then navigate to the certificate to upload it.
   - **Test Credentials:** Click this to validate the Cisco ISE configuration before proceeding. When you click Test Credentials, the appliance validates the certificates.
   - **Comment:** Enter additional information about the configuration.
   - **Disabled:** Select this if you want to save the configuration but do not want to use it yet. You can clear this check box when you are ready to use this Cisco ISE.

3. Click **Next** to specify the data types that you are interested to obtain from the Cisco ISE. The Cisco ISE shares information only for the subscribed data types. Complete the following to specify data types you want to collect from the Cisco ISE:
   - **Subscription Settings:** There are predefined data types in the **Available Data Type** table you can subscribe. Use the arrows to move data types from the **Available Data Type** table to the **Selected Data Type** table and vice versa. The appliance receives information for all data types in the **Selected Data Type** table.
   - **Map other data types to Extensible Attributes:** You can create extensible attributes and map these extensible attributes to receive additional Cisco ISE data values, such as IP address, MAC, NAS IP Address, NAS Port ID, EPS Status, Posture Status, Posture Timestamp, Endpoint Profile Name, Account Session ID, and Audit Session ID. Click the **Add** icon and map a Cisco ISE data type to an extensible attribute. You can also select a row and click the **Delete** icon to delete it.

4. Click **Next** to add extensible attributes to the Cisco ISE. For information, see **About Extensible Attributes**.

5. Save the configuration.

**Modifying Cisco ISE Configurations**

You can select data types that need to be published from NIOS to Cisco ISE after you have configured the Cisco ISE. You can modify the Cisco ISE configurations, as follows:

1. From the **Grid** tab, select the **Ecosystem** tab, and then click the **Add Cisco ISE** from the Toolbar.
2. The Cisco ISE Server editor provides the following tabs from which you can modify data:
   - **General:** You can modify data in this tab as described in **Configuring Cisco ISE on NIOS**.
   - **Subscription:** You can edit data types that you have subscribed. You can use the arrows to move data types from the **Available Data Type** table to the **Selected Data Type** table and vice versa. The appliance receives information for all data types in the **Selected Data Type** table and extensible attributes that are configured.
   - **Publication:** To publish dynamic data from NIOS, you must first configure notification rules, as described in **Configuring Notification Rules**. You can add data types that you want to publish to Cisco ISE server by using the arrows to move data types from the **Available** table to the **Selected** table and vice versa. The appliance publishes information only for the data types that are added in the **Selected** table.
   - **Extensible Attributes:** You can add, modify, and delete extensible attributes that are associated with the Cisco ISE server. For information, see **About Extensible Attributes**.
3. Save the changes.
Overriding Subscription Settings

You can override subscription settings and mapped extensible attributes at the network container, network, and DHCP range levels. By default, networks inherit subscription settings from those configured while adding the Cisco server. You can override these settings and subscribe new values at the DHCP range, network container, or network level. A network inherits subscription settings from its parent object. If you override the values at the network container level, then the network inherits the network container values. Otherwise, the network continues to inherit the values configured from the Cisco ISE. A shared network without a parent network container continues to inherit settings from the Cisco ISE.

To override an inherited value, click Override next to it and complete the appropriate fields. When you click Override, the appliance displays the value inherited from its parent object (if any).

To override subscription settings and mapped extensible attributes:

1. **Network Level**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network check box, and then click the Edit icon.
2. **Network Container**: From the Data Management tab, select the IPAM tab -> network_container check box, and then click the Edit icon.
3. **DHCP Range Level**: From the Data Management tab, select the DHCP tab -> Networks tab -> Networks -> network -> addr_range check box, and then click the Edit icon.

Viewing Identity Mapping Information

To view user information, you must first enable identity mapping feature at the Grid level. For information about enabling Identity Mapping feature, see [Enabling Identity Mapping](#).  

**Note:** You do not need an MS Management license to enable the identity mapping feature.

You can view user information in the Network Users tab. For more information, see [Viewing Identity Mapping Information](#).

Deleting Cisco ISE Servers

When you delete a Cisco ISE, the appliance moves it to the Recycle Bin, if enabled. You can later restore it if needed. To delete a Cisco ISE server:

1. From the Grid tab, select the Ecosystem tab > Cisco tab -> Cisco ISE server check box, and then click the Delete icon.
2. In the Delete Confirmation dialog box, click Yes to delete the Cisco ISE server.

Publishing Data

To publish dynamic data, such as DHCP lease and IPAM information, make sure that you approve Infoblox_DHCP and Infoblox_IPAM on the Cisco ISE, and then configure notification rules as described in [Configuring Notification Rules](#).

To publish RPZ and threat protection notifications to the Cisco ISE server, you must first set up an external syslog server and then configure notification rules, as follows:

1. Configure an external syslog server that listens on port 2000, as described in [Specifying Syslog Server for Notifications](#).
2. Set up notification rules, as described in [Configuring Notification Rules](#).

Specifying Syslog Server for Notifications

Before you can publish RPZ and threat protection notifications to the Cisco ISE, you must first configure the syslog server to which the appliance logs RPZ and threat protection events. The appliance generate notifications about these events and analyze the data before sending it to the Cisco ISE. When setting up the syslog server, ensure that you select DNS RPZ and Threat Protection logging categories so all events related to RPZ and threat protection hits are logged to the syslog.

**Note:** For Cisco ISE to take appropriate action to quarantine malicious IP addresses, ensure that the EPSStatus (Endpoint Protection Status) in the Authorization Policy is set to "Quarantine." This is set by default.

To specify an external syslog server in NIOS, complete the following:

1. From the Grid tab, select the Grid Manager tab -> Members tab, and then click Grid Properties -> Edit from the Toolbar.
2. In the Grid Properties editor, select the Monitoring tab, and then follow the procedures described in [Specifying Syslog Servers](#) using the following settings:
   - Address: Enter the loopback address 127.0.0.1 so the appliance sends notifications to itself.
   - Transport: Select UDP.
   - Interface: Select LAN. The appliance uses the LAN1 port to send syslog messages.
   - Source: Select Any. The appliance sends both internal and external syslog messages.
2. Port: Enter 2000 as the port number.
3. Logging Category: Select DNS RPZ and Threat Protection.

Save the configuration.

Configuring Notification Rules

You can configure notification rules after you have configured Cisco ISE on the NIOS appliance. For information, see Configuring Cisco ISE on Ni OS. To publish data and notifications from NIOS to Cisco ISE, you must configure notification rules. You can create notification rules for the following event types: DNS RPZ, Security ADP, IPAM, and DHCP Lease. Note that the DNS RPZ and Security ADP event types are available only if you have installed RPZ and Threat Protection licenses in the Grid. Each notification rule specifies the target Cisco ISE, the Grid member on which you wish to run this rule, notification rule criteria, and the action to be taken for the matching events. NIOS publishes information, such as DHCP lease information, IPAM data, and quarantine events, when the triggered events matches the notification rule criteria. Note that the DHCP Lease and IPAM event types are available only for the Cisco ISE 2.0 target servers.

Note: Quarantine events are published to the Cisco ISE whenever the first rule matches the trigger criteria and it ignores all other rules.

To add notification rules:

1. From the Grid tab, select the Ecosystem tab -> Notification tab, and then click the Add icon.
   Or
   From the Grid tab, select the Ecosystem tab, and click Add Notification Rule from the Toolbar.

2. In the Add Notification wizard, complete the following:
   - Name: Enter the name of the rule.
   - Target: Select the IP address of the target server on which you want to publish from NIOS. This field displays all the IP addresses of the Cisco servers you have added.
   - Comment: Enter useful information about the notification rule.
   - Disable: Select this option to disable the notification rule.

3. Click Next and complete the following:
   - Event: The appliance displays the list of event types based on the licenses installed. The values in the drop-down list are:
     - DNS RPZ: Select this to create notification rules for the DNS RPZ events.
     - Security ADP: Select this to create notification rules for Security ADP threat events.
     - IPAM Type: Select this to send IPAM data. No notification rule is required for this event type.
     - DHCP Leases: Select this to create notification rules for DHCP Lease events. This is available for Cisco ISE 2.0.
   - In the Match the following rule section, select filters, operators and values from the drop-down lists for the selected event type. You can use the + icon to construct nested expressions within an event category.

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Filters</th>
<th>Operators</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS RPZ</td>
<td>Query Name</td>
<td>equals, begins with, and ends with</td>
<td>Enter the value that you want your rule to match</td>
</tr>
<tr>
<td></td>
<td>Rule Name</td>
<td>equals, begins with, and ends with</td>
<td>Enter the value that you want your rule to match</td>
</tr>
<tr>
<td></td>
<td>Action Policy</td>
<td>equals</td>
<td>Log Only, None, Block No Data, Block No Such Domain, Passthrough, Substitute Domain Name</td>
</tr>
<tr>
<td></td>
<td>Source IP</td>
<td>equals, matches CIDR, matches range</td>
<td>Enter the value that you want your rule to match</td>
</tr>
<tr>
<td>Security ADP</td>
<td>Rule Severity</td>
<td>equals, equal to or more severe, equal to or less severe</td>
<td>Information, Major, Critical, Warning</td>
</tr>
<tr>
<td></td>
<td>SID</td>
<td>contains, equals, begins with and ends with</td>
<td>Enter the value that you want your rule to match</td>
</tr>
<tr>
<td></td>
<td>Rule Message</td>
<td>contains, equals, begins with and ends with</td>
<td>Enter the value that you want your rule to match</td>
</tr>
<tr>
<td></td>
<td>Source IP</td>
<td>equals, matches CIDR, matches range</td>
<td>Enter the value that you want your rule to match</td>
</tr>
<tr>
<td>DHCP Leases</td>
<td>Lease State</td>
<td>equals</td>
<td>Started, Renewed, and Expired</td>
</tr>
</tbody>
</table>

You can override your Publish settings configured for the Cisco ISE server.

- For IPAM and DHCP Lease events: In the Notify the target section, there are predefined data types in the Available table you can publish. Click Override and use the arrows to move data types from the Available table to the Selected table and vice versa.
versa. The appliance sends information for all data types that are added to the Selected table. If you do not override, the publication settings is inherited from those configured while adding the Cisco ISE server. Note that you can configure only one IPAM rule per Cisco ISE server.

- **Action**: The action to be taken for various events. Displays Quarantine the end host for DNS RPZ and Security ADP events.

4. Click **Next** to select Grid members. You can apply this notification rule on specific Grid members or apply this notification rule on all the Grid members.

   - **Apply rule to relevant members**: Select this option to apply notification rule on specific Grid members.
   - **Select Member(s)**: Select this option to select a Grid member for applying the notification rule. If there are multiple members, the Member Selector dialog box is displayed, from which you can select a member. Click the required member name in the dialog box. You can also click **Clear** to clear the displayed member and select a new one.

5. Click **Save** to save the Cisco ISE configuration.

**Examples**

The following illustrations show sample notification rules and how the information is displayed in Grid Manager and the Cisco ISE:

*Figure 44.1 Sample Notification Rule for RPZ Events*

*Figure 44.2 Matching DNS RPZEEvents*
Chapter 45 Ecosystem - Outbound Notifications

This chapter describes how you can use outbound templates to convert NIOS specific events into outbound notifications and send the notifications to REST (REpresentational State Transfer) enabled and DXL (Data Exchange Layer) endpoints. It also explains how to create and add RESTful API and DXL templates that use NIOS specific data to construct outbound notifications, and how to configure notification rules to trigger outbound notifications based on the parameters defined in the templates. It also includes sample templates for supported servers. It includes the following sections:

- Outbound Notification Overview
- Licensing Requirements
- Administrative Permissions
- Best Practices for Outbound Notifications
- About Outbound Templates
  - Creating Session Management Templates
  - Creating Action Templates
  - Action Template Variables and Name Spaces
  - Action Template Variable Format
  - Command Execution
  - Variable Examples
  - Event Variables
  - Result Parsing
  - Adding Outbound Templates
  - Modifying Outbound Templates
  - Viewing Outbound Templates
  - Deleting Outbound Templates
  - Exporting Template Schema
- Configuring Outbound Endpoints
  - Modifying Outbound Endpoints
  - Viewing Outbound Endpoints
- Configuring Notification Rules
  - Adding Notification Rules
  - Deduplicating RPZ Events
  - Selecting Action Template
  - Modifying Notification Rules
  - Viewing All Notification Rules
- Sample Templates
  - Session Management Template
  - Login Template
  - Logout Template
  - Action Template

Outbound Notification Overview
You can use the RESTful API and DXL fabric to obtain core network service information from the Infoblox Grid to assist with profiling the source or destination of network devices or use the RESTful API and WAPI in DXL template to change configurations in the Infoblox Grid to help mitigate security threats. In addition to querying inbound data and changing system configurations and query interfaces, you can use the RESTful API and DXL messages to send outbound notifications so you can prioritize your security needs by detecting new hosts or networks or managing network access control.

When there are serious threats, it is important that you receive notifications so you can address the threats accordingly. On the other hand, you may sometimes need to identify and manage low-risk or accidental threats so the endpoint performance is not negatively affected. For example, if a user inadvertently browses to a faulty web site and you have configured RPZ rules to block this site, you may want to receive notifications and take certain actions so the user is not being blocked or quarantined. In addition, when the Infoblox appliance detects a new host or network, the detection might trigger a vulnerability scan by services such as Qualys and a scan for RPZ events configured in NIOS. In this scenario, you might want to configure conditions to capture these events so you can receive outbound notifications and perform appropriate actions to handle the situation.

To enable outbound API notifications, you must have the Security Ecosystem license installed in your Grid. Depending on the notification rules for RPZ and threat protection event types you want to configure on NIOS, you may need to install the applicable licenses. For information about other licensing requirements, see Licensing Requirements.

The outbound notification feature employs the following mechanism to enable and deliver event-driven messages to configured endpoints:

1. Accepts the configuration of events that you want to monitor (such as RPZ hits) and the configuration of endpoints to which you want to send outbound notifications.
2. Filters events for specific data sets or thresholds, such as RPZ hits for a specific domain within a specific time interval.
3. Matches the selected events and conditions defined in the templates to create outbound messages.
4. Sends outbound notifications to the configured endpoints.

For example, you can first configure RPZ rules to mitigate a malicious IP address, and then configure RESTful API and DXL endpoints to which you want to send the outbound notifications. When configuring your notification rules, you can match RPZ events that are initiated by the RPZ rules and apply the outbound template containing actions to mitigate the threat. The configuration rules then trigger outbound notifications, and the appliance sends the notifications to the configured endpoints and applies the configured actions to combat the offensive IP address. Before you configure the appliance to send outbound notifications, there are a few limitations you might want to consider, as described in Best Practices for Outbound Notifications. For detailed information about how to use the outbound notification feature, see Configuring Outbound Notifications.

Note: To access online resources about this feature, including training videos and sample outbound templates for supported ecosystem partners, ensure that you visit the Infoblox Community Site at [https://community.infoblox.com](https://community.infoblox.com).

For debugging purposes, you can look at the syslog to see if the Outbound service has been started or stopped on specific members. You can also set the logging level to Debug to view all events in the log files, including deduplicated events. However, leaving the logging level at the Debug level could negatively affect your system performance. Therefore, Infoblox does not recommend leaving the logging level at Debug. For information about how to configure the severity level and deduplication, see Configuring Outbound Endpoints.

### Licensing Requirements

You must install the Security Ecosystem license to enable outbound API notifications. After you install the Security Ecosystem license, you can configure REST and DXL endpoints. If you do not have this license installed, the outbound notification feature is disabled. You might also need the following licenses to configure notification rules for certain event types:

<table>
<thead>
<tr>
<th>License</th>
<th>Event Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPZ</td>
<td>DNS RPZ</td>
</tr>
<tr>
<td>DNS and DHCP</td>
<td>DHCP Lease</td>
</tr>
<tr>
<td>Threat Analytics</td>
<td>DNS Tunneling</td>
</tr>
</tbody>
</table>

For information about how to install licenses, see Managing Licenses.

### Administrative Permissions

Only superusers can add, edit, and delete REST endpoints and notification rules by default. Limited-access admin groups can perform these tasks only if their administrative permissions are defined. For information about administrative permissions, see About Administrative Permissions.

### Best Practices for Outbound Notifications

The following are some best practices and limitations you might want to consider while configuring outbound notifications:
• You can configure REST and DXL endpoints only on the Grid Master and Grid Master Candidate, but not on Grid members.
• During a scheduled full upgrade in the Grid, you cannot modify any configuration related to the outbound feature until all Grid members are upgraded.
• Outbound notification is not supported during an HA failover. Any events that are in transit during a failover might be lost.
• When you remove or disable a notification rule, no new events will be triggered. However, the appliance continues to process events that are already in queue.
• The buffer to temporarily hold events are limited and not configurable in this release. In very unlikely conditions, events may be dropped due to a full buffer. If events are dropped, summary information is logged to the syslog to indicate the type of events and the number that have been dropped. If this issue occurs continuously, contact Infoblox Technical Support.
• Events generated due to changes made by admin users do not support the Microsoft Management feature. The appliance does not generate events when there are changes done from the Microsoft servers. However, if you make changes that need to be synchronized to the Microsoft servers, the object change event is generated before the changes are synchronized with the Microsoft servers.
• The Grid Master Candidate will continue to perform event enrichments and outbound API calls during and after a Grid Master promotion.
• If you disable the outbound notification feature or make changes to stop future notifications sent to an endpoint, all notifications that are currently in queue for that endpoint will stop immediately.
• The appliance uses rate limiting to control both data collection from Grid members and outbound notifications to external endpoints. It is possible for the appliance to drop events if its buffer is full or if there is a loss of connection between the Grid Master and the Grid members. Logs for these events are consolidated and logged to the syslog.
• The number of outbound notifications sent to external endpoints can be limited, depending on the requirements configured for the external servers. For example, some REST enabled servers only take 10 API calls per second. Some servers might put a user in suspended mode if the number of API calls sent to the user exceeds the limit. If necessary, you can adjust the rate limit criteria for API calls on the external servers.

**Configuring Outbound Notifications**

To send outbound notifications to an endpoint, you must configure notification rules specifying the target endpoints, notification rule criteria, and the outbound templates you want to use. The REST API endpoint you configure must be REST enabled so they can handle RESTful API calls. The DXL endpoints must be connected to DXL brokers and listen on specific DXL topics as configured in the DXL action template. A notification rule contains the target endpoint to which you want to send outbound notifications and the event type upon which you want to take action. The event type you select in a notification rule must match the event type defined in the template you want to use for that rule. Otherwise, the appliance returns an error. Therefore, you must first create and upload outbound templates to the Grid, and then select the correct template you want to apply to the notification rule.

To configure outbound notifications, complete the following:

1. Prepare outbound templates that you want to use for notification rules. For more information about API templates, see [About Outbound Templates](#). You can also reference sample API templates for supported ecosystem partners and modify them accordingly.

   **Note:** To access online resources about this feature, including training videos and sample API templates for supported ecosystem partners, visit the Infoblox Community Site at [https://community.infoblox.com](https://community.infoblox.com).

2. Upload outbound templates to the Grid so you can use them for corresponding notification rules. For more information, see in [Adding Outbound Templates](#).

3. Configure endpoints to which you want to send outbound notifications. For more information, see [Configuring Outbound Endpoints](#).

4. Select event types and configure criteria for notification rules. For more information, see [Configuring Notification Rules](#).

**About Outbound Templates**

The appliance uses outbound templates to convert NIOS events into REST API and DXL messages. You use supported variables in the templates to get respective events and define actions you want to take for those events. The following are outbound templates you can create. You can also export the schema from the appliance and use it to create the outbound templates. For information about how to export template schema, see [Exporting Template Schema](#). Note that the exported schema is in the IETF JSON Schema format. For information about this schema format, see [https://tools.ietf.org/html/draft-zyp-json-schema-04](https://tools.ietf.org/html/draft-zyp-json-schema-04).

- **Session Management Template**: A session management template contains specific variables about an endpoint, such as the timeout value and rate limiting information. For more information, see [Creating Session Management Templates](#).
- **Action Template**: An action template defines the action(s) to be taken on the selected endpoint for the matching event type(s). It contains scripts the appliance uses to query respective event data from NIOS and to perform actions you want to take in response to the events. For more information, see [Creating Action Templates](#).

After you create your outbound templates, you can do the following to manage them:

- Add outbound templates to the Infoblox Grid, as described in [Adding Outbound Templates](#).
- Modify outbound templates, as described in [Modifying Outbound Templates](#).
- View the list of outbound templates that have been uploaded to the Grid, as described in [Viewing Outbound Templates](#).
- Delete outbound templates, as described in [Deleting Outbound Templates](#).

Copyright ©2019, Infoblox, Inc. All right reserved.
Creating Session Management Templates

You can use a session management template to specify settings that will be applied to an endpoint. You can define settings such as the timeout value after which the outbound requests are aborted. This template can also contain additional child templates that can be referenced by the configuration. However, you cannot reference other templates in the system from the session management template.

Once you upload a session management template to the Grid, the configuration in the template automatically applies to the specified endpoint, if the connection to the endpoint has been established and if the template is assigned to the endpoint.

Table 45.2 lists the supported variables you can use in a session management template.

Note: Changes made to the variables of the template through Grid Manager overrides the variables in the template. Although the latest template version is 3.0, versions 2.0 and 1.0 templates still work fine with version 2.0 and version 1.0 syntax respectively.

Table 45.2 Session Management Template Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>Must be 3.0</td>
<td>Yes</td>
<td>The version number of the template. Note that 3.0 is the latest version. The appliance still fully supports the previous schema version.</td>
</tr>
<tr>
<td>type</td>
<td>Must be REST_ENDPOINT for REST API endpoints Must be DXL_ENDPOINT for DXL endpoints</td>
<td>Yes</td>
<td>The template type.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>Yes</td>
<td>The template name.</td>
</tr>
<tr>
<td>vendor_identifier</td>
<td>String</td>
<td>Yes</td>
<td>The vendor identifier for an endpoint.</td>
</tr>
<tr>
<td>comment</td>
<td>String</td>
<td>No</td>
<td>Additional information.</td>
</tr>
<tr>
<td>path</td>
<td>String</td>
<td>No</td>
<td>Path string to append to what the user enters in the GUI.</td>
</tr>
<tr>
<td>override_path</td>
<td>Boolean</td>
<td>No</td>
<td>If present, the path above replaces the path the user enters in the GUI.</td>
</tr>
<tr>
<td>timeout</td>
<td>Integer</td>
<td>No</td>
<td>The timeout value in seconds. The minimum is 1 and the maximum is 3600. The default is 30.</td>
</tr>
<tr>
<td>keepalive</td>
<td>Boolean</td>
<td>No</td>
<td>The value can be True or False. The default is False.</td>
</tr>
<tr>
<td>keepalive_timeout</td>
<td>Integer</td>
<td>No</td>
<td>The keepalive timeout value in seconds. The connection is closed after this timeout. The minimum is 1 and the maximum is 300. The default is 5.</td>
</tr>
<tr>
<td>dxl_keepalive_timeout</td>
<td>Integer</td>
<td>No</td>
<td>The keepalive timeout value in seconds with a connected DXL broker. This controls the rate at which the client will send ping messages to the broker if there is no exchange of other messages. The minimum is 1 and the maximum is 3600. The default is 30. Note: This field is applicable only for the DXL templates.</td>
</tr>
<tr>
<td>dxl_topic</td>
<td>String</td>
<td>No</td>
<td>The DXL topic that is used to send data by DXL. Note: This variable is applicable only for the DXL templates</td>
</tr>
<tr>
<td>retry</td>
<td>Integer</td>
<td>No</td>
<td>The number of attempts to try to connect to the endpoint before considering the connection a failure (this covers only timeout/network errors). The default value is 2.</td>
</tr>
<tr>
<td>retry_template</td>
<td>Integer</td>
<td>No</td>
<td>The number of attempts the appliance retries the full template if it returns a failure (this covers a template returning anything but 200). The default value is 0 (no retry).</td>
</tr>
<tr>
<td>rate_limit</td>
<td>Float</td>
<td>No</td>
<td>The maximum number of messages (per second) that are sent to an endpoint. The default value is 0 (no rate limiting). You can enter a value less than 1.0 to have lower rate limits. For example, if you set the value to 0.5, the appliance sends less than 1 message in every 2 seconds.</td>
</tr>
<tr>
<td>Variable</td>
<td>Type</td>
<td>Access</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------</td>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>rate_limit_requests</td>
<td>Integer</td>
<td>No</td>
<td>Use this along with rate_limit_interval to define the absolute number of requests for rate limiting. For example, if you set this to 10 and rate_limit_interval to 5000 milliseconds, no further requests are sent until the number of requests falls below 10 in 5000 milliseconds. So if 3 requests are sent at 0 second and 7 requests are sent at the 3rd second, no requests will be sent until the 5th second, where 3 requests are allowed for another 3 seconds. The default is 0 = no rate limiting. You can set this to an integer between 0 and 267840000000.</td>
</tr>
<tr>
<td>rate_limit_interval</td>
<td>Integer (in milliseconds)</td>
<td>No</td>
<td>Use this along with rate_limit_requests to define the rate limiting interval. The default is 0 = no rate limiting. You can set this to an integer between 0 and 267840000000 milliseconds.</td>
</tr>
</tbody>
</table>
| rate_limit_reset         | Integer (in epoch time) | No     | Use this together with rate_limit_requests and rate_limit_interval to reset the epoch time for rate limiting. You can set this to an integer between 0 and 4102437600 milliseconds.  
  Example: If rate_limit_requests = 10, rate_limit_interval = 5 seconds, and rate_limit_reset = 3 p.m. on 10 January 2017 (set in epoch time), 10 requests can be sent within 5 seconds after the reset time.  
  For instance, 3 messages are sent at the 1st second and 7 messages sent at the 3rd second and no more messages can be sent in the next 2 seconds, which is within 5 seconds after 3 p.m. on 10 January 2017. |
| endpoint_variables       | List of VARIABLE structs | No     | If specified these will be accessible via the S: namespace in templates.                                                                                                                                       |
| inactivity_interval      | Integer (in milliseconds) | No     | A logout request is sent after this time interval, provided no other requests have occurred during this time period. The default is 0 = “disable.” You can set this to an integer between 0 and 2^63-1 milliseconds. |
| login_template           | String                | No     | The template that requires user login if there is no active session currently running for the endpoint. Only templates with event_type set to SESSION are supported for this. You must include the template name in the string. Ensure that you upload the login template if you plan to use this variable in the session management template. |
| logout_any_condition     | Boolean               | No     | Specifies whether a logout request is sent, depending on whether logout_status_code or logout_regexp are set. The value can be True or False. The default is False. If this is set to True, a logout request is triggered if either logout_status_code or logout_regexp is set. If this is set to False, both logout_status_code and logout_regexp must be set. |
| logout_regexp            | String                | No     | Any response returned by the endpoint that matches the regular expression in this field will trigger a logout request.                                                                                           |
| logout_status_code       | Integer               | No     | The HTTP response status code used for the provisional response will trigger a logout request. The default is 0 = “disable.” Valid values are between 0 and 599.                                                            |
| logout_template          | String                | No     | The template that is being executed after steps are executed or after various session duration constraints are met. You must include the template name in the string. Only templates with event_type set to SESSION are supported for this. Ensure that you upload the logout template if you plan to use this variable in the session management template. |
| requests_per_session     | Integer               | No     | The number of requests that are sent before a logout request is sent. The default is 0 = “disable.” You can set this to an integer between 0 and 2^63-1.                                                            |
| logout_only_at_template_end | Boolean             | No     | The value can be True or False. The default is False. If this is set to True, a logout request is sent only after the execution of the template has been completed to ensure that all template requests pertaining to a session are executed if that is required by the API. Therefore, it is possible to set requests_per_session to 1 and have each template call executed in its own session regardless of the number of requests it contains. |
| session_cooldown         | Integer (in milliseconds) | No     | When this is set, a login request will be sent only after the amount of time set for this has been elapsed after a logout. The default is 0 = “disable.” You can set this to an integer between 0 and 2^63-1 milliseconds. |
| session_duration         | Integer (in milliseconds) | No     | The time interval after which a logout request is sent unconditionally after a login. For example, if you sent this to 150 milliseconds, after a login, a logout will be sent after 150 milliseconds whether there is current traffic or not. The default is 0 = “disable.” You can set this to an integer between 0 and 2^63-1 milliseconds. |
### Creating Action Templates

The purpose of an action template is to convert an event into one or more RESTful API and DXL messages that are sent from the NIOS appliance to the endpoint configured in the notification rule. An action template consists of a series of statements that are interpreted into specific actions. When creating an action template, ensure that it consists of an initial section with some general template settings, followed by one or more steps that are executed in sequence. Steps are constructed for sending messages to the endpoint and for receiving responses. It can also perform specific operations on template variables.

**Note:** The steps in an action template are executed sequentially. Some constructs enable steps to be skipped by jumping forward in the list of steps; jumping backwards is not supported.

Consider the following guidelines while composing action templates:

- Template error handling is active only if the severity level for logging is set to **Debug**, otherwise error handling is disabled and the server continues to execute a template even if the template tries to access nonexistent variables or perform invalid operations such as trying to increment a STRING variable. For information about setting the severity level for logging, see [Configuring Outbound Endpoints](#). If you have disabled template error handling, then accessing any nonexistent variables will return an empty string and invalid operations are not executed.
- Matching a regular expression is performed un-anchored. If anchoring is required, you must add the characters ^ and/or $ to the respective regular expression.
- For outbound notifications, only template instances are considered. Template instances are constructed from action templates as well as template instance variables in the template. You may configure these variables through Grid Manager when a specific template is associated to an event.

An action template consists of the variables and elements listed in [Figure 45.3](#).

**Note:** When "yes" is indicated in the "Sub" column for a variable, it means that variable substitution (where it is possible to have ${...} variables as part of the value, and have them substituted when the template is executed) is supported for that variable, a * means that the substitution is supported for some of the fields of the struct.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Mandatory</th>
<th>Sub</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>Must be 3.0</td>
<td>No</td>
<td>No</td>
<td>The version number of the template. Note that 3.0 is the latest version. The appliance still fully supports the previous schema version.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>No</td>
<td>No</td>
<td>The template name.</td>
</tr>
<tr>
<td>type</td>
<td>Must be REST_EVENT for REST API endpoints Must be DXL_EVENT for DXL endpoints</td>
<td>No</td>
<td>No</td>
<td>The template type.</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----</td>
<td>----</td>
<td>-------------------</td>
</tr>
<tr>
<td>vendor_identifier</td>
<td>String</td>
<td>No</td>
<td>No</td>
<td>The vendor identifier for an endpoint.</td>
</tr>
<tr>
<td>event_type</td>
<td>List of ENUM (except for SESSION)</td>
<td>Yes</td>
<td>No</td>
<td>Available event types: RPZ, LEASE, TUNNEL, NETWORK_IPV4, NETWORK_IPV6, RANGE_IPV4, RANGE_IPV6, FIXED_ADDRESS_IPV4, FIXED_ADDRESS_IPV6, HOST_ADDRESS_IPV4, HOST_ADDRESS_IPV6, and SESSION. Note that SESSION is used for the login and logout events for the session management templates. For information about supported variables for the session management template, see <a href="#">Session Management Template Variables</a>.</td>
</tr>
<tr>
<td>action_type</td>
<td>String</td>
<td>No</td>
<td>No</td>
<td>The action type.</td>
</tr>
<tr>
<td>comment</td>
<td>String</td>
<td>No</td>
<td>No</td>
<td>Additional information.</td>
</tr>
<tr>
<td>content_type</td>
<td>String</td>
<td>No</td>
<td>No</td>
<td>The content type for the whole template. If not specified, it is set as &quot;application/json&quot;. It can be specified either in the template, inside the transport, or both. If both are specified, then the content type specified in the template takes precedence.</td>
</tr>
<tr>
<td>quoting</td>
<td>ENUM</td>
<td>No</td>
<td>No</td>
<td>Sets the default serialization for template variables. The valid value is one of the following: JSON, XML, XMLA, ASIS, or URL. If not specified, this is set to JSON. To use XMLA for serialization, you must specify a valid quoting for variables. Infoblox strongly recommends that you use XMLA as the quoting option (as opposed to XML) when you create new action templates. New operations such as PUSH, POP, SHIFT and others are not officially supported for XML parsed data.</td>
</tr>
<tr>
<td>headers</td>
<td>Dictionary of key/value pairs</td>
<td>No</td>
<td>Yes</td>
<td>If specified, it is sent for every request of the template, in addition to any other H: namespace variables.</td>
</tr>
<tr>
<td>instance_variables</td>
<td>List of VARIABLE structs</td>
<td>No</td>
<td>No</td>
<td>It must be specified in the GUI to create a template instance.</td>
</tr>
<tr>
<td>template_variables</td>
<td>List of VARIABLE structs</td>
<td>No</td>
<td>No</td>
<td>The template_variables are used when there are common settings in various steps. They are specified for maintainability and they are also available in L: namespace. Note that the template variables are evaluated immediately so that they can be used as reference values in other areas of the template.</td>
</tr>
<tr>
<td>transport</td>
<td>TRANSPORT struct</td>
<td>No</td>
<td>No</td>
<td>It is the default for steps.</td>
</tr>
<tr>
<td>steps</td>
<td>List of STEP structs</td>
<td>No</td>
<td>No</td>
<td>Steps are executed in sequence. You cannot execute them</td>
</tr>
<tr>
<td>step_execution_limit</td>
<td>Integer</td>
<td></td>
<td></td>
<td>The maximum number of times a step can be executed. Steps can be executed more than once if using certain template constructs. To avoid possible endless loops, you can limit an individual step to be executed up to a certain number of times. If a step is executed again after the limit is reached, the execution will be interrupted and a failure is logged. The default is 10. The maximum number is 1000.</td>
</tr>
</tbody>
</table>

**STEP Struct**

Each step can perform a different operation, such as SLEEP, CONDITION, NOP, GET, POST, PATCH, DELETE, DXL_EVENT_SEND, or PUT. Table 45.4 lists the step variables.

**Note:** The name for each step must be unique.

- **SLEEP:** Steps with a SLEEP operation will pause the execution for the number of seconds specified in the timeout parameter.
- **NOP:** Steps with a NOP operation will only parse the text specified in body/body_list without sending it to the endpoint. This can be useful for executing operations on variables to prepare data for subsequent steps.
- **CONDITION:** Steps with a CONDITION operation will cause a condition specified in statements to be matched. See Table 45.10 for information about condition variables and Table 45.11 for statement variables.

If the condition matches, the execution of the template will do the following:

- Stop without errors if the stop field is present,
- Stop with an errors if the error field is present,
- Jump forward to the specified step if the next field is present,
- and/or evaluate the text in eval if the field is present.

If the condition does not match, the text in the else_eval field will be evaluated instead, if the field is present.

- GET, POST, PATCH, DELETE, and PUT: These steps will result in an endpoint communication. The request will be sent to an URI composed by the URI configured in the endpoint, plus the path configured in the session management template if present (or replaced by it, depending on its override setting), plus the path configured in the event template if present (same override considerations), plus the path configured in the individual step if present (same override considerations).

  After variable substitution, any data present in the H: namespace will be sent as headers, any parameters listed will be sent as URI parameters, and any data in body/body_list will be sent as the body of the request. Note also that each step can override the endpoint timeout. This is useful when a certain operation is known to require a longer execution time.

  If the result variable is set in the step, the reply from the server will be evaluated and compared against the specified codes and/or REGEX, and the operation specified in the result step will be executed.

  If parse is set in the step, the result from the server will also be parsed and be made available in the P: namespace as described above.

### Table 45.4 STEP Structs

**Note:** Set the "wapi" field to send WAPI requests to the Grid Master using available event data. For example, you can add or modify extensible attributes of a NIOS object at the time when the object is being synchronized. If you include the "wapi" field in a step, you must enable WAPI integration by entering the WAPI login username and password while configuring the endpoint. Otherwise, the WAPI step will fail due to an authorization error. For information about how to configure endpoints, see Configuring Outbound Endpoints.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Mandatory</th>
<th>Sub</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Yes</td>
<td>No</td>
<td>Used to refer to the steps used in the execution of the template.</td>
</tr>
<tr>
<td>operation</td>
<td>ENUM</td>
<td>Yes</td>
<td>No</td>
<td>The valid value can be one of the following: GET, POST, DELETE, PATCH, PUT, SLEEP, CONDITION, NOP, VARIABLEOP, DXL_EVENT_SEND, or SERIALIZE. If you specify SLEEP, only timeout is supported, where timeout is the sleep length in seconds. If you specify NOP, only variable operations are performed, and only body/body_list is supported. If you specify VARIABLEOP, you must use the VARIABLE struct within your steps that are executed in sequence. See VARIABLE Struct for the supported fields. If you specify SERIALIZE, see SERIALIZE Struct for the supported variables.</td>
</tr>
<tr>
<td>condition</td>
<td>CONDITION Struct</td>
<td>No</td>
<td>No</td>
<td>Applicable only if the operation is set to CONDITION.</td>
</tr>
<tr>
<td>timeout</td>
<td>String</td>
<td>No</td>
<td>Yes</td>
<td>If specified, overrides the endpoint configuration value (it is useful if the template is slow during execution). Note that the timeout value is invalid for NOP. Since the timeout variable is a string, you can substitute the variable in individual steps.</td>
</tr>
<tr>
<td>transport</td>
<td>TRANSPORT Struct</td>
<td>No</td>
<td>Path only</td>
<td></td>
</tr>
<tr>
<td>result</td>
<td>List of RESULT Structs</td>
<td>No</td>
<td>No</td>
<td>If not present, you can assume 200, everything else is a failure. If not specified, the steps are executed sequentially. This is not valid for SLEEP, NOP, or CONDITION variables.</td>
</tr>
<tr>
<td>parse</td>
<td>ENUM</td>
<td>No</td>
<td>No</td>
<td>If specified, the output of the server will be parsed. The valid value is one of the following: JSON, REGEXLINE, REGEXMULTILINE, REGEX, XMLA, or XML. Infoblox recommends that you use XMLA instead of XML for parsing. Ensure that you see Result Parsing for details.</td>
</tr>
<tr>
<td>parse_regex</td>
<td>String</td>
<td>No</td>
<td>No</td>
<td>You can set one of the following: REGEX, REGEXLINE, or REGEXMULTILINE</td>
</tr>
<tr>
<td>parameters</td>
<td>List of PARAMETERS</td>
<td>No</td>
<td>Value only</td>
<td>These are URI parameters.</td>
</tr>
<tr>
<td>headers</td>
<td>Dictionary of name/value pairs</td>
<td>No</td>
<td>Yes</td>
<td>This is sent as HTTP headers. The name space substitution is supported only for value. Note that assigning to the H: name space also sends headers.</td>
</tr>
<tr>
<td>override_headers</td>
<td>Boolean</td>
<td>No</td>
<td>No</td>
<td>If specified, only these headers and H: name space headers are sent instead of template headers.</td>
</tr>
<tr>
<td>body</td>
<td>String</td>
<td>No</td>
<td>Yes</td>
<td>This is applicable only for POST, PATCH, DXL_EVENT_SEND, and PUT requests as well as NOP operations. It will be sent as the body of the request. Note that name space substitution is supported.</td>
</tr>
<tr>
<td>body_list</td>
<td>List of strings</td>
<td>No</td>
<td>Yes</td>
<td>This is an alternative to the body. If specified, the strings in the list will be joined before sending it. Any leading or trailing whitespace is removed.</td>
</tr>
<tr>
<td>no_connection_debug</td>
<td>Boolean</td>
<td>No</td>
<td>No</td>
<td>The valid value is True or False. If this is set to True even if the endpoint is set to a Debug level logging, only the body, headers, and cookies for the corresponding step will NOT be output to the debug log. Only explicit DEBUG calls will be displayed. This is generally used in login templates to avoid usernames and passwords from being logged to the log files in plain text.</td>
</tr>
</tbody>
</table>
### VARIABLEOP Struct

**Note:** All variables listed in the following table are applicable only for the VARIABLEOP operation in the STEP struct. The VARIABLEOP struct converts specified keys/values in a complex variable (such as LIST, DICTIONARY, or XML values with attributes) or performs operations on an existing complex variable. No schema validation is made for variable combinations. Validation of the schema is performed when you add or modify the action template.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Mandatory</th>
<th>Sub</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>String</td>
<td>No</td>
<td>Yes</td>
<td>You must specify the variable name, including the namespace. Example: L:DICT[key][list]</td>
</tr>
<tr>
<td>destination</td>
<td>String</td>
<td>No</td>
<td>Yes</td>
<td>You must specify the variable name, including the namespace. Example: L:DICT[key][list]</td>
</tr>
<tr>
<td>operation</td>
<td>ENUM</td>
<td>Yes</td>
<td>Yes</td>
<td>Specifies the operation being performed for the value defined or created in type. The valid value is one of the following: PUSH, POP, SHIFT, UNSHIFT, or ASSIGN. Note that both operation and type are mandatory for the struct. For examples, see Using OPERATION in the VARIABLE Struct.</td>
</tr>
</tbody>
</table>
| type       | ENUM           | Yes       | Yes  | Specifies the type of variables for the operation. Valid value is one of the following: LIST, DICTIONARY, COMPOSITE, or SINGLE. This field defines how the values in keys, values, and composite_value are combined to create a variable while operation defines how the variable is being used. The appliance handles keys, values and composite_value differently based on the type you select, as follows:  
  - LIST: keys will be ignored; values will contain the required values and be serialized in a simple list of strings.  
  - DICTIONARY: The list of key/value pairs in keys and values will be put in a simple dictionary.  
  - COMPOSITE: The list of key/value pairs in keys and values will be put in an XMLA dictionary with a name set to name and a value set to either the value in composite_value OR to the value in the variable set in source. See Using the COMPOSITE Type for details about how to use COMPOSITE.  
  - SINGLE: Keys will be ignored; the value will be the first element in the values list. |
| name       | String         | No        | Yes  | This is applicable only if you select COMPOSITE as the variable type. Enter the name value for this type. |
| keys       | List of strings | No       | Yes  | This can contain arbitrary serializable constructs. |
| values     | List of strings | No       | Yes  | This can contain arbitrary serializable constructs. When you specify this field inside any variable operation for the VARIABLEOP step type, it is possible to use the constant of a specific type, instead of using string. For details about how to specify type, instead of using string. For details about how to use constant, see Constant Specification for values. |
| composite_value | String       | No       | Yes  | This can contain arbitrary serializable constructs. |
| destination_key | String       | No       | Yes  | This can contain arbitrary serializable constructs. |
| if_exists  | ENUM           | No        | Yes  | The action taken if the variable exists. The valid value is one of the following: SKIP, ERROR, or NEXT. |
| if_exists_next | String       | No        | Yes  | Enter the name for the next step. |
| condition  | CONDITION Struct | No   |      | This can be specified for POP and UNSHIFT operations. |

### Using the COMPOSITE Type

When you use COMPOSITE as the type in the VARIABLE struct, the list of key/value pairs in keys and values is put in an XMLA dictionary with a name set to name and a value set to either the value in composite_value OR to the value in the variable set in source.
Here is an example of using COMPOSITE as the type when you use the following variables and values:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>COMPOSITE</td>
</tr>
<tr>
<td>name</td>
<td>varname</td>
</tr>
<tr>
<td>keys</td>
<td>['a1', 'a2']</td>
</tr>
<tr>
<td>values</td>
<td>['value is ${L::SOMEVAR}', '2']</td>
</tr>
<tr>
<td>composite_value</td>
<td>&quot;123&quot;</td>
</tr>
</tbody>
</table>

It results in the following:

```json
{
    "<xmla>": true,
    "attrs": {
        "a1": "value is 123",
        "a2": "2",
    },
    "index": {},
    "value": ["123"],
    "name": "varname"
}
```

**Note:** If source is set, the value in source is used as is (this can be seen especially for PUSH operations).

**Using OPERATION in the VARIABLE Struct**

**operation ASSIGN**

If operation is set to ASSIGN, the value in type will be simply put in the variable identified by destination, overwriting any value it might already have.

The following are several examples of the ASSIGN operation having namespace E as follows:

```json
{
    'some_field': 'some_value',
    'some_list': ['item1', 'item2']
}
```

(1) When assigning a single value:

```json
{
    'operation': 'ASSIGN',
    'type': 'SINGLE',
    'destination': 'L:var',
    'values': ['value']
}
```

It returns name space L as follows:

```json
{'var': 'value'}
```

(2) When assigning a list:
(3) When assigning a dictionary:

```json
{
  'operation': 'ASSIGN',
  'type': 'DICTIONARY',
  'destination': 'L:dict',
  'keys': ['$E:A:some_field_1', '$E:A:some_field_2'],
  'values': ['$E:A:some_list[0]', '$E:A:some_list[1]']
}
```

It returns the following:

```json
{'dict': {'some_value_2': 'item2', 'some_value_1': 'item1'}}
```

(4) When assigning a composite value, as follows:

```json
{
  'operation': 'ASSIGN',
  'type': 'COMPOSITE',
  'destination': 'L:composite',
  'name': 'tag_name',
  'keys': ['attr_1', 'attr_2'],
  'values': ['$E:A:some_field', 'another_value'],
  'composite_value': 'tag_content'
}
```

It gives the following:

```json
{'composite': {
  'index': {}, '<xmla>': True,
  'attrs': {
    'attr_2': 'another_value',
    'attr_1': 'some_value'
  },
  'value': ['tag_content'],
  'name': 'tag_name'
}}
```

This composite value can be serialized to the following XML:

```
<tag_name attr_1="some_value" attr_2="another_value">tag_content</tagname>
```
**operation PUSH and SHIFT without setting if_exists**

If `destination_key` is set, the assumption is to push or shift to a dictionary; otherwise, it is to push or shift to a list.

For pushing to a list, if the `destination` variable exists and is a list, the list of values in `values` will be added to the existing list. With PUSH, it means that the values will be added to the right side of the list (at the end) of the list. With SHIFT however, the values will be added to the left side (at the beginning) of the list.

If the `destination` variable is a dictionary, it will be converted to a list that contains only one element with the value appended to it. This means that for XML deserializing and JSON values, it is possible to create a list by pushing it on to an existing scalar value.

For pushing to a dictionary, it means that with `destination_key` set, if the `destination` variable exists and is anything but a dictionary, it is considered as an error. If it is a dictionary however, the value above will be added with its key set to `destination_key` overwriting any existing value.

If the variable denoted by `destination` has a composite value, the COMPOSITE type can be pushed or shifted to it only. If the destination composite value contains text, the text will be replaced with the composite value. In other cases, the PUSH operation using the new value will be added to the right side of the children list. For the SHIFT operation, the new value will be added to the left side of the children list.

The following are several examples of the `ASSIGN` operation having namespace E:

```json
{
'operation': 'PUSH',
'type': 'SINGLE',
'destination': 'L:some_list',
'values': ['$E:A:some_field_right'],
}
```

and namespace L as follows:

```json
{
    'some_list': ['item1', 'item2'],
    'some_dict': {'key': 'val'},
    'compl': {
        'index': {}, '<xmla>': True,
        'attr1_b': 'another_value',
        'attr1_a': 'some_value'
    },
    'value': ['tag_1_content'],
    'name': 'tag_1'
},
'comp2': {
    'index': {}, '<xmla>': True,
    'attr1_b': 'another_value',
    'attr1_a': 'some_value'
}
```

(1) When PUSH or SHIFT to a list:
'It returns namespace L as the following:

{
'some_list': [['left_some_value'], 'item1', 'item2', 'some_value_right']
}

(2) When PUSH or SHIFT to a dictionary, it returns the following:

{'some_dict': {
  'push1': 'item',
  'push2': ['item_1', 'item_2'],
  'key': 'val'
}}

Note: There is no difference between PUSH and SHIFT when destination is DICTIONARY.

(3) When PUSH or SHIFT to a composite value:

{  
  'operation': 'PUSH',
  'type': 'COMPOSITE',
  'destination': 'L:comp1',
  'name': 'pushed',
  'composite_value': ''
},

{  
  'operation': 'SHIFT',
  'type': 'COMPOSITE',
  'destination': 'L:comp1',
  'source': 'L:comp2'
}

It returns the following:

{  
  'comp1': {
    'index': {u'pushed': 1, 'tag_2': 0},
    '<xmla>': True,
    'attrs': {'attr1_a': 'some_value', 'attr1_b': 'another_value'},
    'value': [
      {'index': {}, '<xmla>': True, 'attrs': {}, 'value': ['tag_2_content'], 'name': 'tag_2'},
      {'index': {}, '<xmla>': True, 'attrs': {'attr': 'val'}, 'value': [], 'name': 'pushed'}
    ],
    'name': 'tag_1'
  }
}
Note that the first operation (PUSH) overwrites existing value and the second operation (SHIFT) shifts the value to the existing list. This composite value can be serialized to the following XML:

```xml
<tag_1 attr1_a="some_value" attr1_b="another_value">
  <tag_2>tag_2_content</tag_2>
  <pushed attr="val"/>
</tag_1>
```

**operation PUSH and SHIFT with if_exist set**

If `destination_key` is set, the assumption is to push or shift to a dictionary. Otherwise it is to push or shift to a list.

If you are pushing to a list, and the variable already exists, the operation specified there will be executed as follows: SKIP will not modify the original value, NEXT will not modify and jump to the step specified in `if_exists_next`, and ERROR will instead return an error.

If you are pushing to a dictionary, and the variable matches, there is no need to modify the values because they would already be the same. Therefore, SKIP will be a no-operation, NEXT will not modify and jump to the step specified in `if_exists_next`, and ERROR will instead return an error.

The decision for whether a new value exists or not is a simple comparison with the value/attributes of the existing variables in the list or dictionary in `destination_key`. They all have to match for `if_exists` for the operation to be triggered.

If variable denoted by `destination_key` has a composite value, the semantics is as above, with additional checks. The check is complete before the value is added to the list of children. During the check, the new composite value is compared one by one with the existing values. If the values are the same, the "if_exists" logic is triggered as above.

The following are a few examples using namespace L as follows:

```json
{
    'some_list': ['item1', 'item2'],
    'some_dict': {'key1': 'val1', 'key2': 'val2'},
    'list_of_lists': [['a', 'b'], ['a', '2'], ['1', '2']],
    'composite': {
        '<xmla>': True,
        'index': {'inner_1': 0, 'inner_2': 1},
        'name': 'outer',
        'attrs': {'outer_attr': 'outer_val'},
        'value': [
            {
                '<xmla>': True,
                'index': {},
                'name': 'inner_1',
                'attrs': {},
                'value': ['inner_1_content']
            },
            {
                '<xmla>': True,
                'index': {},
                'name': 'inner_2',
                'attrs': {'inner_attr': 'inner_val'},
                'value': []
            }
        ]
    }
}
```
(1) When PUSH to a list with the item exists:

```json
{
    'operation': 'PUSH',
    'type': 'SINGLE',
    'destination': 'L:some_list',
    'values': ['item2'],
    'if_exists': 'ERROR'
}
```

It triggers the 'if_exists' login. 'ERROR' means stopping the template execution with error, 'SKIP' means 'do nothing for this operation' and 'NEXT' will jump to the step with name specified in 'if_exists_next'.

(2) When PUSH to a dictionary with the item exists:

```json
{
    'operation': 'PUSH',
    'type': 'SINGLE',
    'destination': 'L:some_dict',
    'destination_key': 'key2',
    'values': ['val2'],
    'if_exists': 'ERROR'
}
```

It triggers an error. Note that both key and value should be the same in order to trigger the 'if_exists' logic. If key is the same but value differs, value will be overwritten. If key is different, the new key with value will be added.

(3) When PUSH to a list of list with the item exists:

```json
{
    'operation': 'PUSH',
    'type': 'LIST',
    'destination': 'L:list_of_lists',
    'values': ['a', '2'],
    'if_exists': 'ERROR'
}
```

It triggers an error.

(4a) When PUSH to a composite value with the item exists, as follows:

```json
{
    'operation': 'PUSH',
    'type': 'COMPOSITE',
    'destination': 'L:composite',
    'name': 'inner_1',
    'composite_value': 'inner_1_content',
}
```
It triggers an error.

(4b) When PUSH to a composite value with the item exists, as follows:

```json
{
    'operation': 'PUSH',
    'type': 'COMPOSITE',
    'destination': 'L:composite',
    'name': 'inner_2',
    'keys': ['inner_attr'],
    'values': ['inner_val'],
    'composite_value': '',
    'if_exists': 'ERROR'
}
```

It triggers an error.

**operation POP and UNSHIFT**

If the source variable is anything but a dictionary, a list, or a composite value, an error is returned. If keys is set, the source value is assumed to be a dictionary. Otherwise, an error is returned.

If the source variable is a list, a single value is removed from the list. If the operation is POP, it is removed from the right side (from the end). If the operation is UNSHIFT, it is removed from the left (at the beginning). The removed value is put in the destination variable.

If the source variable is a composite value, the operation is on the children list of the composite value. Note that it is not possible to POP or UNSHIFT from a composite value, if it has text only.

If the source variable is a dictionary, the specified keys and/or key/value pairs will be removed from the variable in source. If only keys are passed, those keys will be unconditionally removed. If keys and values are passed, the key will be removed from the source variable only if its value matches what is passed in values here. If only one key or key/value pair is passed, the removed value will be put in destination. Otherwise, it will simply be dropped.

For the values match, the value in the list or dictionary will be serialized with quoting specified in the template before being compared to the string value passed in values. This also means that using comparison on large lists would potentially be a slow operation.

In the POP or UNSHIFT case, type is validated to be the same as the type of the popped or unshifted variable (you can validate if they were planning to pop a simple scalar if there is one). If it is not, an error will be raised if debug is turned on.

The following are a few examples using namespace L as follows:

```json
{
    'some_list': ['item1', 'item2'],
    'some_dict': {'key1': 'val1', 'key2': 'val2'},
    'list_of_lists': [['a', 'b'], ['1', '2']],
    'list_of_dicts': [{'a': '1'}, {'b': '2'}],
    'composite': {
        '<xmla>': True,
        'index': {'inner_1': 0, 'inner_2': 1},
        'name': 'outer',
        'attrs': {'outer_attr': 'outer_val'},
        'value': [
            
```
(1) When POP from a list:

```
{  
    "operation": "POP",
    "type": "SINGLE",
    "source": "L:some_list",
}
```
It gives the variable as follows:
```
{"some_list": ["item1"]}
```

(2) When UNSHIFT from a list:

```
{  
    "operation": "UNSHIFT",
    "type": "SINGLE",
    "source": "L:some_list",
}
```
It returns the following:
```
{"some_list": ["item2"]}
```

(3) When UNSHIFT from a dict by key:

```
{  
    "operation": "UNSHIFT",
    "type": "SINGLE",
    "source": "L:some_dict",
    "keys": ["key1"]
}
```
It returns the following:
```
{"some_dict": {"key2": "val2"}} There is no difference between POP/UNSHIFT fro dictionarries
(4) When POP from a dict by multiple keys:

```
{
    "operation": "POP",
    "type": "SINGLE",
    "source": "L:some_dict",
    "keys": ["key1", "key2"]
}
```

It returns the following:

```
{"some_dict": {}}
```

(5) When POP from a dict when a key is absent:

```
{
    "operation": "POP",
    "type": "SINGLE",
    "source": "L:some_dict",
    "keys": ["key1", "absent_key"]
}
```

It returns an error in the DEBUG mode. For non-DEBUG mode, all existing keys are POPed. Note that items are popped one by one, so key1 item is popped before the error is returned.

```
{"some_dict":{"key2": "val2"}}
```

(6) When POP from composite value:

```
{
    "operation": "POP",
    "type": "SINGLE",
    "source": "L:composite",
}
```

It returns the following:

```
{
    "composite": {
        "index": {"inner_1": 0},
        "<xmla>": True,
        "name": "outer",
        "value": [{
            "index": {},
            "<xmla>": True,
            "name": "inner_1",
            "value": ["inner_1_content"],
            "attrs": {}
        }],
        "attrs": {"outer_attr": "outer_val"}
    }
}
```
This can be serialized to the following:

```xml
<outer outer_attr="outer_val">
    <inner_1>inner_1_content<inner_1>
</outer>
```

(7) When conditional POP/UNSHIFT from a list:

```
{
    "operation": "POP",
    "type": "SINGLE",
    "source": "L:some_list",
    "values": ["item1"]
}
```

It returns the following:

```json
{"some_list": ["item2"]}
```

There is no difference between POP and UNSHIFT when `values` is specified. When source is either **LIST** or **COMPOSITE**, all occurrences of a value are deleted.

(8) When conditional POP/UNSHIFT from a dictionary:

```
{
    "operation": "UNSHIFT",
    "type": "SINGLE",
    "source": "L:some_dict",
    "keys": ["key2"],
    "values": ["val2"]
}
```

It returns the following:

```json
{"some_dict": {"key1": "val1"}}
```

(9) When conditional POP/UNSHIFT of multiple values:

```
{
    "operation": "UNSHIFT",
    "type": "SINGLE",
    "source": "L:some_dict",
    "keys": ["key2", "key2"],
    "values": ["abc", "val2"]
}
```

It returns the following:

```json
{"some_dict": {"key1": "val1"}}
```

(10) When conditional POP/UNSHIFT with list values:

```
{
    "operation": "POP",
    "type": "SINGLE",
    "source": "L:list_of_lists",
    "values": ["\"[1, '2']\"]
}
```
It returns the following:

```json
{"list_of_lists": [["a", "b"]]}  
```

For conditional POP/UNSHIFT, non-string values are serialized with the template's quoting. For JSON, quoting is added to value.

(11) When conditional POP/UNSHIFT with dictionary value:

```json
{  
  "operation": "POP",
  "type": "DICTIONARY",
  "source": "L:list_of_dicts",
  "values": ["\"{\"b\": \"2\"}\"]
}
```

It returns the following:

```json
{"list_of_dicts": ["{\"a\": \"1\"}"]}
```

(12a) When conditional POP/UNSHIFT with the following composite values:

```json
{  
  "operation": "POP",
  "type": "COMPOSITE",
  "source": "L:composite",
  "values": ["\"{\"index\": {}, \"<xmla>\": True, \"name\": \"inner_2\", \"value\": [], \n  
  \t\"attrs\": {\"inner_attr\": \"inner_val\"}}\"]
}
```

It returns the following:

```json
{
  "composite": {
    "index": {"inner_1": 0},
    "<xmla>": True,
    "name": "outer",
    "value": [{
      "index": {},
      "<xmla>": True,
      "name": "inner_1",
      "value": ["inner_1_content"],
      "attrs": {}
    }],
  "attrs": {"outer_attr": "outer_val"}
  
```

(12b) When conditional POP/UNSHIFT with the following composite values, and with the template quoting set to XMLA, the example in (12a) can be specified as follows:

```json
{  
  "operation": "POP",
  "type": "COMPOSITE",
  "source": "L:composite",
  "values": ["\"{\"index\": {}, \"<xmla>\": True, \"name\": \"inner_2\", \"value\": [], \n  
  \t\"attrs\": {\"inner_attr\": \"inner_val\"}}\"]
}
```

```json
{
  "composite": {
    "index": {"inner_1": 0},
    "<xmla>": True,
    "name": "outer",
    "value": [{
      "index": {},
      "<xmla>": True,
      "name": "inner_1",
      "value": ["inner_1_content"],
      "attrs": {}
    }],
  "attrs": {"outer_attr": "outer_val"}
  
```

Copyright ©2019, Infoblox, Inc. All right reserved.
Type check after POP/UNSHIFT:

```
{
  "operation": "POP",
  "type": "LIST",
  "source": "L:some_dict",
  "keys": ["key2"]
}
```

It returns an error in the DEBUG mode. Since the type of POPed value is not LIST, the possible values for type are 'SINGLE', 'LIST', 'DICTIONARY', and 'COMPOSITE', where 'SINGLE' means 'no check'. Note that type check is done after the item is retrieved from source. In the DICTIONARY case, when several keys are specified, there is no type check. Type check is done after value comparison.

(13) When putting the item to 'destination' :

```
{
  "operation": "POP",
  "type": "COMPOSITE",
  "source": "L:composite",
  "destination": "L:sub_item"
}
```

It returns the following:

```
{
  "composite": {
    "index": {"inner_1": 0},
    "<xmla>": True,
    "name": "outer",
    "value": [
      {"index": {}, "<xmla>": True, "name": "inner_1", "value": ["inner_1_content"],
        "attrs": {}}
    ],
    "attrs": {"outer_attr": "outer_val"}
  },
  "sub_item": {
    "index": {},
    "<xmla>": True,
    "name": "inner_2",
    "value": [],
    "attrs": {"inner_attr": "inner_val"}
  }
}
```
If the value popped/unshifted from source and destination is specified, the value is written to the destination. The value is written after the type check.

The L:sub_item can be serialized as the following:

\[ <inner_2 inner_attr="inner_val"/> \]

**Constant Specification for values**

When you specify the `values` field inside any variable operation for the VARIABLEOP step type, it is possible to use the constant of a specific type, instead of string.

For example, the following describes three string values:

```javascript
'values': ['True', '42', '{}L::some_var']
```

If you specify `values` as `'{X:something}'`, `something` is represented as a constant of type X. Note that this is the only allowed syntax. For example, `text{X:something}` is treated as a string, instead of a constant specification.

The following types are supported in constant specification:

- **Bool type (B):** Both '{B:1}' and '{B:true}' are evaluated as bool true, while '{B:0}' and '{B:false}' are evaluated as bool false. Note that both 'true' and 'false' are not case-sensitive. Therefore, True, FALSE or even tRuE are all allowed. Other invalid values such as 'B:' and '{B:anythingelse}' are evaluated as bool=false (the 'default value') without further debugging; and an error is logged in the debug mode.

- **Integer type (I):** '{I:}' is evaluated to its corresponding integer value. For example, '{I:-42}' is evaluated as integer -42. The default value is 0.

- **Empty type (E):** '{E:}' is evaluated as None. '{E:[]}' is evaluated as an empty list. '{E:{}}' is evaluated as an empty dictionary. The default value is None.

- **Float type (F):** The float type is similar to the integer type. Float numbers can be specified as '{F:0.0}', '{F:-4.2}', '{F:-4E+2}' or '{F:+1.23e-45}'. The default value is 0.0.

- **String type (S):** '{S:}' is evaluated as string '. For example, '{S:42}' is string '42'. There is no default value for string. For the unknown type (e.g. '{U:%^&}'), the default value is an empty string.

The following example illustrates how to use constant specification to define ipv4addr with a DHCP option:

```javascript
{
  "ipv4addr": "1.2.3.4",
  "options": [
    {
      "name": 'dhcp-lease-time",
      "num": 51,
      "use_option": true,
      "value": '43200",
      'vendor_class': "DHCP"
    }
  ]
}
```

Note that `num` is an integer (in this string: "num": "51") and `use_option` is bool (in this string: "use_option": "true").

In the action template, you can do the following:

```javascript
{
  "steps": [
    {
      "operation": 'VARIABLEOP",
      "variable_ops": [
        {
          "operation": "ASSIGN",
```
"type": "DICTIONARY",
"destination": "L:addr",
"keys": ["ipv4addr", "options"],
"values": ["1.2.3.4", "{E:[]}"]
},
{
"operation": "PUSH",
"type": "DICTIONARY",
"destination": "L:addr{options}"",
"keys": ["name", "num", "use_option", "value", "vendor_class"],
"values": ["dhcp-lease-time", "{I:51}", "{B:true}", "43200", "DHCP"]
}
}
,
{
"operation": "PUT",
"transport": {"path": "record:host_ipv4addr"},
"body": "${L:J:addr}"
}
]
]
,
{
"operation": "PUT",
"transport": {"path": "record:host_ipv4addr"},
"body": "${L:J:addr}"
}
]

Table 45.6 SERIALIZE Struct

Note: All variables listed in the following table are applicable only for the SERIALIZE operation in the STEP struct. The SERIALIZE structs inside the step are executed in sequence.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Mandatory</th>
<th>Sub</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>content</td>
<td>String</td>
<td>Yes</td>
<td>Yes</td>
<td>Defines what to serialize. This can contain arbitrary variables and text.</td>
</tr>
<tr>
<td>destination</td>
<td>String</td>
<td>Yes</td>
<td>Yes</td>
<td>Defines the destination for the serialization.</td>
</tr>
</tbody>
</table>

TRANSPORT Struct

Table 45.7 TRANSPORT Structs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Mandatory</th>
<th>Sub</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path</td>
<td>String</td>
<td>No</td>
<td>Yes, if specified in step.</td>
<td>If present, it is appended to the endpoint URI.</td>
</tr>
<tr>
<td>override_path</td>
<td>Boolean</td>
<td>No</td>
<td>No</td>
<td>If this is true, the specified path completely overrides the endpoint URI after the first <code>/</code>.</td>
</tr>
<tr>
<td>content_type</td>
<td>String</td>
<td>No</td>
<td>No</td>
<td>If specified, this overrides the endpoint content type.</td>
</tr>
</tbody>
</table>

RESULT Struct

Note the following:
- `codes` and `regex` are ignored if the operation is SLEEP or NOP.
- At least one of the following is required: `next`, `stop`, or `error`.

Table 45.8 RESULT Structs
<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Mandatory</th>
<th>Sub</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>codes</td>
<td>comma separated int list</td>
<td>No</td>
<td>No</td>
<td>The http return code</td>
</tr>
<tr>
<td>regex</td>
<td>REGEX</td>
<td>No</td>
<td>No</td>
<td>If specified, REGEX is matched against the returned body.</td>
</tr>
<tr>
<td>next</td>
<td>id</td>
<td>No</td>
<td>No</td>
<td>The step to execute the next template if the code (and REGEX, if specified) match. But if the next template is already executed once, the appliance displays an error.</td>
</tr>
<tr>
<td>stop</td>
<td>Boolean</td>
<td>No</td>
<td>No</td>
<td>If set, the execution of the script is stopped. Note that next, error, and stop are mutually exclusive.</td>
</tr>
<tr>
<td>error</td>
<td>Boolean</td>
<td>No</td>
<td>No</td>
<td>If set, the execution of the script is stopped and then rerun with an error status if the retry_template is not set to 0. Note that next, error, and stop are mutually exclusive.</td>
</tr>
</tbody>
</table>

**PARAMETER Struct**

**Table 45.9** PARAMETER Structs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Mandatory</th>
<th>Sub</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Yes</td>
<td>No</td>
<td>Name of the parameter.</td>
</tr>
<tr>
<td>value</td>
<td>String</td>
<td>Yes</td>
<td>Yes</td>
<td>Value of the parameter. Note that this value is used as-is, so any strings that are not part of the variables must be URL encoded (%20 for spaces, and etc.)</td>
</tr>
</tbody>
</table>

**CONDITION Struct**

**Table 45.10** CONDITION Structs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Mandatory</th>
<th>Sub</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>condition_type</td>
<td>String</td>
<td>Yes</td>
<td>No</td>
<td>This can be one of the following: AND, OR, NAND, or NOR. NAND means not (st1, st2, etc.)</td>
</tr>
<tr>
<td>next</td>
<td>String</td>
<td>No</td>
<td>No</td>
<td>The name of the step to jump to if the condition is successful.</td>
</tr>
<tr>
<td>eval</td>
<td>String</td>
<td>No</td>
<td>Yes</td>
<td>This is executed if the condition is successful. Generally, it will be an XC: set of operations.</td>
</tr>
<tr>
<td>else_eval</td>
<td>String</td>
<td>No</td>
<td>Yes</td>
<td>This is executed if the condition is NOT successful. Generally, it will be an XC: set of operations.</td>
</tr>
<tr>
<td>else_next</td>
<td>String</td>
<td>No</td>
<td>Yes</td>
<td>The execution will jump to specified step if the condition is NOT successful.</td>
</tr>
<tr>
<td>else_stop</td>
<td>String</td>
<td>No</td>
<td>Yes</td>
<td>The template execution will be stopped if the condition is NOT successful.</td>
</tr>
<tr>
<td>else_error</td>
<td>String</td>
<td>No</td>
<td>Yes</td>
<td>Generates an error if the condition is NOT successful.</td>
</tr>
<tr>
<td>stop</td>
<td>Boolean</td>
<td>No</td>
<td>No</td>
<td>If the condition is successful the execution will be stopped without any error.</td>
</tr>
<tr>
<td>error</td>
<td>Boolean</td>
<td>No</td>
<td>No</td>
<td>If the condition is successful the execution will be stopped with an error.</td>
</tr>
<tr>
<td>statements</td>
<td>List of STATEMENT structs</td>
<td>Yes</td>
<td>Yes</td>
<td>The statements to evaluate.</td>
</tr>
</tbody>
</table>

**STATEMENT Struct**

**Table 45.11** STATEMENT Structs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Mandatory</th>
<th>Sub</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>left</td>
<td>String</td>
<td>Yes</td>
<td>Yes</td>
<td>The left operand. Note that it is acceptable to include variables that do not exist on the left side (to test if a variable is set in an event). Any error during evaluation of the &quot;left&quot; is ignored even if it is run under debug mode.</td>
</tr>
<tr>
<td>op</td>
<td>ENUM</td>
<td>Yes</td>
<td>No</td>
<td>The operation to execute. This can be one of the following: =, &gt;, &lt;, &gt;=, &lt;=, =<del>, and !</del>. Note that the &gt;, &gt;=, and &lt;= operations try to convert the operands to numbers before executing the comparison, then =<del>, and !</del> are REGEX matches and the right side is considered the REGEX.</td>
</tr>
</tbody>
</table>
Action Template Variables and Name Spaces

Action templates can access variables in several different name spaces. The following are the available name spaces:

- **C**: http cookies. It supports only the DEL operation (primarily for logout purposes), but it can be used as a substitution origin.
- **Read-Only E**: Event data.
- **H**: http headers. Note that the assigned variables are sent in the next HTTP request and it survives the template execution.
- **Read-Only I**: Template instance variables. It is set in the GUI during the creation of the filter and it also includes the endpoint variables that are set in the GUI when creating an endpoint. Note that the instance variables can override endpoint variables, if needed.
- **L**: Local template variables. This name space is empty at name space startup and will not survive the template invocation.
- **Read-Only P**: Previous endpoint response values (if parsing is enabled for the response.)
- **Read-Only R**: Previous endpoint request http-specific return values. This includes RC, the http status code of the previous request (Example: 200), BODY, and the body of the response.
- **Read-Only RH**: Previous endpoint request that returned http headers.
- **S**: Endpoint session state variables. These variables survive the template invocation (it is used similar to L: name space which is not cleared at the end of the template execution.)
- **Read-Only UT**: Read-only utility variables. The UT: name space contains the following read-only variables:
  - **EPOCH**: EPOCH seconds since Jan 1st, 1970 (integer, 1 second resolution.)
  - **UUID**: Random UUID of the form 00000000-0000-0000-0000-000000000000.
  - **PROTOCOL**: The protocol used for the request.
  - **URI**: Complete URI used for the request.
  - **HOST**: The endpoint address.
  - **PORT**: The port used for the request.
- **Read-Only XC**: Execute a command on the variable. This results no output.

Action Template Variable Format

The following sequences are substituted with dynamic data:

\${<data namespace>:<output format>:<name of the data or operation dependent values>}

The sequences cannot contain the following characters as variable names: {, }, [ and ]. Therefore, if names contain keys of dictionary/EA variables, they must be quoted with the \ character. Example: "${{E::SOME_EA{name with \ embedded \ braces or brackets}}". But if the \ character is desired, it must be quoted as \\ Note that variable substitution happens only once, it is not nested (i.e. if the value contains $\{...}, it will not be recursively substituted). Also, the dynamic data is not supported for instance and template variables which are assumed to be immediate values.

The following types of variables allow further qualifiers after the variable name. The qualifiers are always mandatory. Therefore, if a variable is a list or a dictionary, then you must specify [ ] or { }.

- **EA** (Extensible Attribute) variables or dictionaries. In general, you must specify [EName] for EA variables or dictionaries. For example, if you specify $[E::NETWORK_EA{City}], it means the city EA from the network EAs. Note that data specific portion is mandatory for EA variables.
- **List variables.** You can specify the list index using square brackets. For example, for a list of DNS names if you specify $[E::DNS_NAMES[0]], this indicates the first DNS name in the list.

You can also use { } or [ ] to signify the full dictionary or list that is supported only in some encodings. Optionally, you can specify the output format. The following output formats are supported:

- **J**: The output is in the form of JSON formatted variable. It supports deserializing lists as well as dictionaries. Note that strings will have double quotes prepended/appended when serialized with J.
- **j**: The output is in the form of JSON formatted variable. It supports deserializing lists as well as dictionaries without the leading or trailing double quotes, if the variable is a string.
- **X**: The output is in the form of XML formatted variable. It supports deserializing lists, such as < item >... </item > sequence.
- **U**: The output is in the form of url encoded variable. It supports deserializing lists and the output will be a string (comma separated value.)
- **A**: The output will be a variable, which is as-is.
- **S**: The output is in the form of a string. This is the default for JSON if you do not specify any output format. By default, even numbers will be serialized as JSON strings, meaning the output in a JSON quoted template for a numerical value of 1234 will be "1234".
- **N**: The output is in the form of numbers. For example, if the variable is a boolean, the output will be 0, 1, etc.
- **B**: The output will be a boolean, that is true/false.
- **L**: The length of the variable. This is supported only for lists (the length of the list) and dictionaries (the number of keys).
- **T**: The type of the variable. This can be one of the following characters: ‘S’ for strings, ‘L’ for lists, ‘D’ for dictionaries, ‘B’ for booleans, ‘N’ for numbers, and ‘O’ for otherwise.

The default is set by the template quoting option and by using a variable. If you have not set the template quoting, then JSON will be set, by default. If you have set the template quoting, the output format will be as specified, unless the variable is in the following fields:
**Command Execution**

If you use XC: name space, then the value can be one of the following:

**Note:** The argument will be one or two nested variable specifications separated by `:` but without the `$` symbol. The variables inside 'XC' do not have an output format, so you must use only one `:`.

- **ASSIGN**: Assigns the value to the specified variable. Note that the value assigned is in the format I/S/B:value for integer, string, and boolean values. Example: ASSIGN:variable:value.
- **DEBUG**: Outputs the specified variable to the debug file (if the log level is not set to DEBUG, this will be ignored), if only the name space is used, the whole name space will be printed.
- **INC**: Increments the variable value. If the value is not a number, NIOS displays an error.
- **DEC**: Increments the variable value. If the value is not a number, NIOS displays an error.
- **COPY**: Copies one variable into another. Example: COPY:destination:source.
- **DEL**: Removes the variable. This supports only the C:, H:, L:, and S: name spaces.
- **FORMAT**: Formats the value according to what is specified after the second `:`. Currently, NIOS supports the following formats:
  - **U**: Converts to uppercase value.
  - **L**: Converts to lowercase value.
  - **DATE_EPOCH**: Assuming that the value is a date expressed in UTC ISO 8601 date format. For example, 2016-03-13T04:50:31Z will be converted to EPOCH seconds.
  - **DATE_ISO8601**: Assuming that the value contains EPOCH seconds. The value is converted to a date string expressed in UTC ISO 8601 date format. For example, 1467152565 will be converted to 2016-06-28T22:45Z. If the variable contains milliseconds, they will be preserved. For example 1467152565.57 will be converted to 2016-06-28T22:45:57Z.
  - **DATE_STRFTIME**: Assuming that the variable contains EPOCH seconds. The value is converted to a date string with the specified format which is passed as the second parameter to the function.
  - **PUNYCODE_TO_UTF-8**: Assuming that the variable contains a punycode encoded domain name. The domain name representation will be converted to UTF-8 characters. Note that there might be a failure if the domain name has non-UTF-8 characters in its wire format.
  - **TRUNCATE**: Assuming that the variable is a string and it will be truncated as specified. The format is a number (positive or negative) followed by the letter 'f' or 'r'. The number is the starting character of the string (positive will be counted from the beginning, negative will be counted from the end) and 'f' defines if the characters are from, after, or to that point. For example, if a string is 12345, then 1f will produce 2345, 1t will produce 1, -1f will produce 5 and -1t will produce 1234.

Format operations will function like other operations if an error occurs, but the variable is not modified. However, the error can be ignored if the log setting is not set to Debug. For information about how to set the logging level, see Configuring Outbound Endpoints.

The following are some examples of using XC operations to increment and decrement IP address strings, create a network range, or remove a specific IP address.

**Incrementing or Decrementing IP addresses**

Use the **INC** and **DEC** operations respectively to increment and decrement IP address strings.

**Examples:**

- For namespace `{L:{'ip_str': '1.2.3.4'}}, an evaluating variable '#{XC:DEC:{L:ip_str}}' results in `{L:{'ip_str': '1.2.3.3'}}.
- The same goes for IPv6 addresses. For namespace `{L:{'ip_str': '2001:db8::2}}`, an evaluating variable '#{XC:INC:{L:ip_str}}' results in `{L:{'ip_str': '2001:db8::3'}}`, and an evaluating '#{XC:DEC:{L:ip_str}}' results in `{L:{'ip_str': '2001:db8::1'}}`.

The increment of the last address results in the first address. The decrement of the first address results in the last address.

**Examples:**

- INC of `255.255.255.255` results in `0.0.0.0`
- DEC of `0.0.0.0` results in `255.255.255.255`

**Creating Network Ranges from Strings**

Use the **NETWORKTORANGE** operation to create a range from a network string. This operation should be specified as the following: `{XC:NETWORKTORANGE:{var_with_network}:{var_for_range}}` where network is a string such as `1.2.3.4/16` or `2001:db8:ce4::/48`.

The resulting range is an XMLA value such as the following:

```xml
{
  '<xmla>': True,
  'name': 'range',
}```
or

```json
{
    '<xmla>': True,
    'name': 'range',
    'value': [],
    'index': {}
}
```

**Note:** "Var_with_network" must be a top-level variable in a namespace such as E:var, but not L:var[key][42].

When namespace E is `{E: {net: '1.2.3.4/16'}}` and the response is as follows:

```
<SiteConfigResponse success="1">
    <Site id="42" name="this_site" description="testing site" riskfactor="1.0" isDynamic="0">
        <Description>testing site</Description>
        <Hosts>
            <host>a.com</host>
        </Hosts>
        <Credentials></Credentials>
        <Alerting></Alerting>
        <ScanConfig configID="21" name="CIS" templateID="cis" engineID="3" configVersion="3">
            <Schedules></Schedules>
        </ScanConfig>
    </Site>
</SiteConfigResponse>
```

Then using the following steps:

```json
{
    "name": "copy",
    "operation": "NOP",
    "body_list": [
        "${XC:COPY:{L:Site}:{P:PARSE{SiteConfigResponse}}}",
        "${XC:NETWORKTORANGE:{E:net}:{L:range}}"
    ],
},
{
    "name": "add",
    "operation": "VARIABLEOP",
    "variable_ops": [
        {
            "operation": "PUSH",
            "type": "COMPOSITE",
            "destination": "L:Site{Site}{Hosts}",
            "source": "L:range"
        }
    ],
},
{
    "name": "post",
    "operation": "POST",
    "body_list": [
        '<?xml version="1.0" encoding="UTF-8"?>',
        '<SiteSaveRequest session-id="some_sess_id"',
        '${L:x:Site}',
        '</SiteSaveRequest>'
    ]
}
```
Removing Specific IP Addresses from Hosts or Ranges

Use the `XC:REMOVEIP` operation to remove a specific IP address from a list of hosts or ranges. This operation should be specified as the following: `$(XC:REMOVEIP:{"var_with_ip"}::{"var_with_list"})` where IP address is a string such as `'1.2.3.4'` or `'2001:db8:ce4::42'`.

The list of hosts/ranges is as follows:

```json
[
  {
    '<xmla>': True,
    'name': 'range',
    'attrs': {'from': '1.2.3.1', 'to': '1.2.3.7'},
    'value': [],
    'index': {}
  },
  {
    '<xmla>': True,
    'name': 'host',
    'attrs': {},
    'value': [a.com],
    'index': {}
  }
]
```

**Note:** "var_with_IP" must be a top-level variable in a namespace such as `E:var`, but not `L:var{key}[42]`.

Having namespace `E` as `{ 'E': { 'ip': '1.2.3.4' } }` and Rapid7 response as follows:

```xml
<SiteConfigResponse success="1">
  <Site id="42" name="this_site" description="testing site" riskfactor="1.0" isDynamic="0">
    <Description>testing site</Description>
    <Hosts>
      <host>a.com</host>
      <range from="1.2.3.1" to="1.2.3.7"/>
      <host>b.com</host>
    </Hosts>
    <Credentials/>
    <Alerting/>
    <ScanConfig configID="21" configVersion="3" name="CIS" templateID="cis" engineID="3">
      <Schedules/>
    </ScanConfig>
  </Site>
</SiteConfigResponse>
```

Use the following steps:

```json
{
  "name": "copy",
  "operation": "NOP",
  "body_list": [
```

Copyright ©2019, Infoblox, Inc. All rights reserved.
It returns the following XML results:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<SiteSaveRequest session-id="some_sess_id">
  <Site name="this_site" isDynamic="0" description="testing site" riskfactor="1.0" id="42">
    <Description>testing site</Description>
    <Hosts>
      <host>a.com</host>
      <range from="1.2.3.1" to="1.2.3.3"/>
      <range from="1.2.3.5" to="1.2.3.7"/>
      <host>b.com</host>
    </Hosts>
    <Credentials/>
    <Alerting/>
    <ScanConfig configID="21" configVersion="3" name="CIS" templateID="cis" engineID="3">
      <Schedules/>
    </ScanConfig>
  </Site>
</SiteSaveRequest>
```

**XC:Remove* Operations**

There are several XC:REMOVE* operations that can be used to remove one or more IP specified addresses from a list of hosts and ranges. Such list is the deserialized representation of the 'Hosts' element of the Rapid7 response or request.

For example,

```json
[
  {
    '<xmla>': True,
    'name': 'host',
    'attrs': {},
    'value': ['a.com'],
    'index': {}
  },
  {
    '<xmla>': True,
    'name': 'range',
    'attrs': {'from': '1.2.3.1', 'to': '1.2.3.7'},
    'value': [],
    'index': {}
  },
  {
    '<xmla>': True,
    'name': 'host',
    'attrs': {},
    'value': ['b.com'],
    'index': {}
  }
]
```

Represents the following "Hosts" element:
<Hosts>
    <host>a.com</host>
    <range from="1.2.3.1" to="1.2.3.7"/>
    <host>b.com</host>
</Hosts>

Items in the list are iterated one by one upon execution of any REMOVE command. The first argument of the REMOVE* command is the variable specification that contains an IP address. The second argument is the variable with the list of ranges or hosts. If the item is 'range', then the specified IP address is deleted from the range. Execution of any REMOVE command may result in no range, one range or two ranges that do not contain any specified IP addresses. The IP addresses specified in non-range items and ranges with different IP addresses are ignored. The XC:REMOVEIP command specifies the single IP address as string (for example, '1.2.3.4' or '2001:db8:ce4::42'). The XC:RMEOVERANGE command specifies the set of IP addresses as Rapid7 range. The XC:REMOVENET command specifies the set of IP addresses as network string. If the first argument denotes an incorrect IP address (range or network respectively), the template execution is stopped and an error is generated for DEBUG mode, and nothing happens for non-DEBUG mode.

**Evaluating IP Address in a Range or Network**

Use the XC:IS_IP_IN operation to validate if an IP address is in the range and network. This operation should be specified as follows: ${XC:IS_IP_IN:{"var_with_IP"}::{"var_with_net_or_range"}} where IP address is a string such as '1.2.3.4' or '2001:db8:ce4::42'.

Having the L namespace as:

```json
{
    'ip1': '1.2.3.4',
    'ip2': '2001:db8:ce5::42',
    'range': {
        '<xmla>': True,
        'name': 'range',
        'attrs': {'from': '1.2.0.0', 'to': '1.2.255.255'},
        'value': [],
        'index': {} },
    'net': '2001:db8:ce4::/48'
}
```

The ${XC:IS_IP_IN:{L:ip1}:{L:range}} variable will be evaluated to string as "true".
The ${XC:IS_IP_IN:{L:ip2}:{L:net}} variable will be evaluated to string as "false".

**Creating Keys**

Use the XC:KEYS operation to create keys. This operation should be specified as follows: ${XC:KEYS:{"var_with_dict"}::{"var_for_key_list"}}. It creates a list from the keys of the 'var_with_dict' variable and includes it in the 'var_for_key_list' variable.

Having L namespace as

```json
{
    'some_dict': {
        'key1': 'value',
        'key2': 42,
        'key3': ['item1', 'item2']
    }
}
```

After evaluating the ${XC:KEYS:{L:some_dict}:{L:key_list}} variable, the L namespace will contain new variable key_list with the following values:

```json
[ 'key1',
  'key2',
  'key3'
]
```

**Variable Examples**

The following are variable examples.

**Note:** The XC: examples refer to the operations discussed in the Command Execution section.
### Variables and Results

<table>
<thead>
<tr>
<th>Variable:</th>
<th>Result:</th>
</tr>
</thead>
<tbody>
<tr>
<td>${E::FQDN}</td>
<td>Substitute the FQDN value from the event.</td>
</tr>
<tr>
<td>${I::QUARANTINE}</td>
<td>Substitute the quarantine value from the template instance.</td>
</tr>
<tr>
<td>${XC:COPY:{E:TIMESTAMP}:{L:epoch_timestamp}}${XC:FORMAT:DATE_EPOCH:{L:epoch_timestamp}}</td>
<td>Copy the event TIMESTAMP value into a local epoch_timestamp variable.</td>
</tr>
<tr>
<td>${XC:COPY:{E:TIMESTAMP}:{L:custom_timestamp}}${XC:FORMAT:DATE_STRFTIME:{L:custom_timestamp}:{%a, %d %b %Y %H:%M:%S}}</td>
<td>Copy the event TIMESTAMP value to a local custom_timestamp variable and format it. In this example, the result might be Wed, 18 Jun 2015 16:13:11.</td>
</tr>
<tr>
<td>${XC:INC:{S:SERIAL}}${S::SERIAL}</td>
<td>Increment the state ‘SERIAL’ value and substitute its value</td>
</tr>
<tr>
<td>${XC:COPY:{S:SERIAL}:{H:X-customheader}}</td>
<td>Copy the state SERIAL value to a custom HTTP header for future requests</td>
</tr>
<tr>
<td>${XC:DEL:{H:X-loginvalue}}</td>
<td>Removes the specified HTTP header.</td>
</tr>
<tr>
<td>${XC:DEL:{C:logincookie}}</td>
<td>Removes the specified cookie.</td>
</tr>
<tr>
<td>${XC:ASSIGN:{L:INT}:{I:123}}</td>
<td>Assign the integer 123 to the value INT in the L name space.</td>
</tr>
<tr>
<td>${XC:ASSIGN:{L:BOOL}:{B:true}}</td>
<td>Assign true to the value BOOL in the L name space.</td>
</tr>
<tr>
<td>${XC:ASSIGN:{L:STR}:{S:some } random string}</td>
<td>Assign the string some } random string to the value STR in the L name space.</td>
</tr>
<tr>
<td>${XC:DEBUG:{L:INT}}</td>
<td>Output the value of the L name space INT variable to the debug file.</td>
</tr>
<tr>
<td>${XC:DEBUG:{L:}}</td>
<td>Output the values in the whole L name space to the debug file.</td>
</tr>
<tr>
<td>${XC:FORMAT:TRUNCATE:{L:VAR}:{-1f}}</td>
<td>Truncate L:VAR to the last character.</td>
</tr>
</tbody>
</table>

### Event Variables

The E: event name space is populated with variables from the event. For performance reasons, only the variables referred in the template will be available in the name space. This means that if the template is changed and if a new variable is added, it might take some time for the changes to be propagated to all the Grid members and the new variable to be available in future template executions.

You can use event_type in an action template to specify the following supported event types: RPZ, LEASE, TUNNEL, NETWORK_IPV4, NETWORK_IPV6, RANGE_IPV4, RANGE_IPV6, FIXED_ADDRESS_IPV4, FIXED_ADDRESS_IPV6, HOST_ADDRESS_IPV4, HOST_ADDRESS_IPV6, and SESSION. Note that SESSION is used only for the login and logout events for the session management templates. For information about action templates, see Creating Action Templates; and for information about session management templates, see Creating Session Management Templates.

The following tables list the supported variables by event type:

*Table 45.12 Variables for RPZ Events*
<table>
<thead>
<tr>
<th>NIOS Field Name</th>
<th>Template Variable Name</th>
<th>Supported Filter(s)</th>
<th>Enriched Data</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>timestamp (ISO 8601 format)</td>
<td></td>
<td></td>
<td>The timestamp when the event occurred.</td>
</tr>
<tr>
<td>Infoblox Member IP</td>
<td>member_ip</td>
<td></td>
<td></td>
<td>Infoblox Member IP (VIP or LAN1) that generated this event.</td>
</tr>
<tr>
<td>Infoblox Member Name</td>
<td>member_name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action Policy</td>
<td>rpz_policy</td>
<td>equals</td>
<td></td>
<td>(PASSTHRU DROP TCP-ONLY NXDOMAIN NODATA Local-Data CNAME MISS)</td>
</tr>
<tr>
<td>RPZ Type</td>
<td>rpz_type</td>
<td>equals</td>
<td></td>
<td>Possible values: BAD, CLIENT-IP, QNAME, IP, NSDNAME, NSIP</td>
</tr>
<tr>
<td>Query Name or Query FQDN</td>
<td>query_name</td>
<td>contains, equals, begins with, ends with</td>
<td>Parent range, Associated objects’ DNS Names and EAs, Parent Network, Parent Network EA, Discovered data</td>
<td></td>
</tr>
<tr>
<td>Rule Name</td>
<td>rule_name</td>
<td>contains, equals, begins with, ends with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source IP</td>
<td>source_ip</td>
<td>equals, matches range, matches CIDR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Port</td>
<td>source_port</td>
<td></td>
<td></td>
<td>The name server that responded to the RPZ rule.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>destination_ip</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Query Type</td>
<td>query_type</td>
<td></td>
<td>DNS query type: A, AAAA, CNAME, DNAME, TXT, and other.</td>
<td></td>
</tr>
<tr>
<td>Query View Name</td>
<td>query_view_name</td>
<td></td>
<td>Query DNS view name.</td>
<td></td>
</tr>
<tr>
<td>Event Type</td>
<td>event_type</td>
<td>equals</td>
<td></td>
<td>SESSION is used for the login and logout events for the session management templates.</td>
</tr>
</tbody>
</table>

**Enriched from IPv4 or IPv6 Addresses**

<table>
<thead>
<tr>
<th>Source IP User Name</th>
<th>ip.username</th>
<th>From IPv4Address and IPv6Address</th>
<th>This field can be empty.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Associated EA</td>
<td>ip.extattrs</td>
<td>From IPv4Address and IPv6Address pyabs class</td>
<td>Can be empty, EA needs to be stored as “name-value” pair.</td>
</tr>
<tr>
<td>Source IP Associated DNS Names</td>
<td>ip.names</td>
<td>From IPv4Address or IPv6Address</td>
<td>List of FQDN</td>
</tr>
</tbody>
</table>

**Enriched from Discovered Data**
| Source IP Attached Device Model | ip.discovered_data.device_model | From discovered data |
| Source IP Attached Device Name | ip.discovered_data.device_port_name | From discovered data |
| Source IP Attached Device Port | ip.discovered_data.device_port_type | From discovered data |
| Source IP Attached Device Type | ip.discovered_data.device_type | From discovered data |
| Source IP Attached Device Vendor | ip.discovered_data.device_vendor | From discovered data |
| Source IP Discovered Name | ip.discovered_data.discovered_name | From discovered data |
| Source IP First Discovered | ip.discovered_data.first_discovered (ISO 8601 format) | From discovered data |
| Source IP Discovered MAC | ip.discovered_data.mac_address | From discovered data |
| Source IP NetBIOS Name | ip.discovered_data.netbios_name | From discovered data |
| Source IP Port Link | ip.discovered_data.port_link_status | From discovered data |
| Source IP Port Speed | ip.discovered_data.port_speed | From discovered data |
| Source IP Port Status | ip.discovered_data.port_status | From discovered data |
| Source IP VLAN Description | ip.discovered_data.port_vlan_description | From discovered data |
| Source IP VLAN Name | ip.discovered_data.port_vlan_name | From discovered data |

**Enriched from Parent Range**

| Source IP Range Start Address | range.start_addr | From parent range |
| Source IP Range End Address | range.end_addr | From parent range |

**Enriched from Parent Network**

| Source IP Network View Name | network.network_view | From parent network |
| Source IP Network | network.network | From parent network |
| Source IP Network Address | network.ipv4addr | From parent network | ip_addr/cidr |
| Example: 1.2.3.4/24 |
| Source IP Network Cidr | network.netmask | From parent network | cidr |
| Source IP Network EA | network.extattrs | From parent network | EA name can be any UTF8 characters. |

**Enriched from Lease Data**

| Source IP Lease Start Time | lease.starts (ISO 8601 format) | From lease data |
### Table 45.13 Variables for DHCP Lease Events

When searching for DHCP lease events with associated discovered data, both the "address" and "hardware" or "duid" must match the discovered data. If there is no hardware or DUID, the lease event cannot be associated with any discovered data.

For leases, same IP addresses may be used by multiple systems, so the IP address must match the MAC address or DUID to ensure that the discovered data has the most likely correct value.

<table>
<thead>
<tr>
<th>NIOS Field Name</th>
<th>Template Variable Name</th>
<th>Supported Filter</th>
<th>Enriched Data</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>timestamp (ISO 8601 format)</td>
<td></td>
<td></td>
<td>The timestamp when the event occurs.</td>
</tr>
<tr>
<td>Infoblox Member IP</td>
<td>member_ip</td>
<td>.</td>
<td></td>
<td>Infoblox member IP (VIP or LAN1) that has generated the event</td>
</tr>
<tr>
<td>Infoblox Member Name</td>
<td>member_name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lease Binding State</td>
<td>binding_state</td>
<td>equals</td>
<td>Parent Network EA, Parent Range, DNS Names and EA of associated objects</td>
<td>Some information from parent network is already in the DHCP lease data.</td>
</tr>
<tr>
<td>Lease IP address</td>
<td>address</td>
<td>equals, matches range, matches CIDR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lease Protocol</td>
<td>protocol</td>
<td></td>
<td>Possible values are IPv4 or IPv6.</td>
<td></td>
</tr>
<tr>
<td>Lease Start Time</td>
<td>starts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lease End Time</td>
<td>ends</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client MAC address</td>
<td>hardware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client IPv6 DUID</td>
<td>ipv6_duid</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Host Name</td>
<td>client_hostname</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td>contains, equals, begins with, ends with</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lease Network View Name</td>
<td>network_view</td>
<td>contains, equals, begins with, ends with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lease Network</td>
<td>network</td>
<td>ip_addr/cidr</td>
<td>Example: 1.2.3.4/24</td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------</td>
<td>---------------</td>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td>Lease Network Address</td>
<td>network_ipaddr</td>
<td>ip_addr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lease Network CIDR</td>
<td>network_netmask</td>
<td>CIDR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lease IP Range Start Address</td>
<td>range_start_addr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lease IP Range End Address</td>
<td>range_end_addr</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Event Type            | event_type | equals | RPZ  
LEASe  
TUNNEL  
NETWORK_IPV4  
NETWORK_IPV6  
RANGE_IPV4  
RANGE_IPV6  
FIXED_ADDRESS_IPV4  
FIXED_ADDRESS_IPV6  
HOST_ADDRESS_IPV4  
HOST_ADDRESS_IPV6  
SESSION  | SESSION is used for the login and logout events for the session management templates. |

**Enriched from Network EA**

| Lease Network EA       | network.extattrs | From parent network EA | EA name can be any UTF-8 characters. |

**Enriched from IPv4 Address and IPv6 Address**

<table>
<thead>
<tr>
<th>Lease IP Username</th>
<th>ip.username</th>
<th>From IPv4 Address and IPv6 Address</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lease IP Associated EA</td>
<td>p.extattrs</td>
<td>From IPv4 Address and IPv6 Address</td>
<td>EA must be stored as &quot;&lt;EA name&gt;-&lt;EA value&gt;&quot; pair.</td>
</tr>
<tr>
<td>Lease IP Associated DNS Names</td>
<td>ip.names</td>
<td>From IPv4 Address and IPv6 Address</td>
<td>List of FQDN</td>
</tr>
</tbody>
</table>

**Enriched from Discovery Data**

<table>
<thead>
<tr>
<th>Lease IP Attached Device Model</th>
<th>ip.discovered_data.device_model</th>
<th>From discovered data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lease IP Attached Device Name</td>
<td>ip.discovered_data.device_port_name</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Lease IP Attached Device Port</td>
<td>ip.discovered_data.device_port_type</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Lease IP Attached Device Type</td>
<td>ip.discovered_data.device_type</td>
<td>From discovered data</td>
</tr>
<tr>
<td>NIOS Field Name</td>
<td>Template Variable Name</td>
<td>Supported Filter</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Lease IP Attached Device Vendor</td>
<td>ip.discovered_data.device_vendor</td>
<td></td>
</tr>
<tr>
<td>Lease IP Discovered Name</td>
<td>ip.discovered_data.discovered_name</td>
<td></td>
</tr>
<tr>
<td>Lease IP First Discovered</td>
<td>ip.discovered_data.first_discovered (ISO 8601 format)</td>
<td></td>
</tr>
<tr>
<td>Lease IP Discovered MAC</td>
<td>ip.discovered_data.mac_address</td>
<td></td>
</tr>
<tr>
<td>Lease IP NetBIOS Name</td>
<td>ip.discovered_data.netbios_name</td>
<td></td>
</tr>
<tr>
<td>Lease IP Port Link</td>
<td>ip.discovered_data.port_link_status</td>
<td></td>
</tr>
<tr>
<td>Lease IP Port Speed</td>
<td>ip.discovered_data.port_speed</td>
<td></td>
</tr>
<tr>
<td>Lease IP Port Status</td>
<td>ip.discovered_data.port_status</td>
<td></td>
</tr>
<tr>
<td>Lease IP VLAN Description</td>
<td>ip.discovered_data.port_vlan_description</td>
<td></td>
</tr>
<tr>
<td>Lease IP VLAN Name</td>
<td>ip.discovered_data.port_vlan_name</td>
<td></td>
</tr>
</tbody>
</table>

**Table 45.14 Variables for Analytics DNS Tunneling Events**

<table>
<thead>
<tr>
<th>NIOS Field Name</th>
<th>Template Variable Name</th>
<th>Supported Filter</th>
<th>Enriched Data</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>timestamp (ISO 8601 format)</td>
<td></td>
<td></td>
<td>When the event occurs</td>
</tr>
<tr>
<td>Infoblox Member IP</td>
<td>member_ip</td>
<td>equals, matches range, matches CIDR</td>
<td>Parent Network, Parent Network EA, Discovery</td>
<td>Infoblox member IP (VIP or LAN1) that has generated the event.</td>
</tr>
<tr>
<td>Infoblox Member Name</td>
<td>member_name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source IP</td>
<td>source_ip</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Name</td>
<td>domain_name</td>
<td></td>
<td></td>
<td>Domain name that was determined as DNS tunneling domain.</td>
</tr>
<tr>
<td>RPZ Rule Policy</td>
<td>rpz_policy</td>
<td>equals</td>
<td></td>
<td>RPZ rule policy that was created.</td>
</tr>
<tr>
<td>Event Type</td>
<td>event_type</td>
<td>equals</td>
<td></td>
<td>SESSION is used for the login and logout events for the session management templates.</td>
</tr>
<tr>
<td>Comment</td>
<td>comment</td>
<td>Comment generated from the event by the Analytics system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Enriched from IPv4 Address or IPv6 Address**

<table>
<thead>
<tr>
<th>Source IP Username</th>
<th>ip.username</th>
<th>From IPv4 Address and IPv6 Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Associated EA</td>
<td>ip.extattrs</td>
<td>From IPv4 Address and IPv6 Address pyabs class</td>
</tr>
<tr>
<td>Source IP Associated DNS Names</td>
<td>ip.names</td>
<td>From IPv4 Address and IPv6 Address</td>
</tr>
</tbody>
</table>

**Enriched from Discovery Data**

<table>
<thead>
<tr>
<th>Source IP Attached Device Model</th>
<th>ip.discovered_data.device_model</th>
<th>From discovered data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Attached Device Name</td>
<td>ip.discovered_data.device_port_name</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Source IP Attached Device Port</td>
<td>ip.discovered_data.device_port_type</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Source IP Attached Device Type</td>
<td>ip.discovered_data.device_type</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Source IP Attached Device Vendor</td>
<td>ip.discovered_data.device_vendor</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Source IP Discovered Name</td>
<td>ip.discovered_data.discovered_name</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Source IP First Discovered</td>
<td>ip.discovered_data.first_discovered (ISO 8601 format)</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Source IP Discovered MAC</td>
<td>ip.discovered_data.mac_address</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Source IP NetBIOS Name</td>
<td>ip.discovered_data.netbios_name</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Source IP Port Link</td>
<td>ip.discovered_data.port_link_status</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Source IP Port Speed</td>
<td>ip.discovered_data.port_speed</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Source IP Port Status</td>
<td>ip.discovered_data.port_status</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Source IP VLAN Description</td>
<td>ip.discovered_data.port_vlan_description</td>
<td>From discovered data</td>
</tr>
<tr>
<td>Source IP VLAN Name</td>
<td>ip.discovered_data.port_vlan_name</td>
<td>From discovered data</td>
</tr>
</tbody>
</table>

**Enriched from Parent Range**

<table>
<thead>
<tr>
<th>Source IP Range Start Address</th>
<th>range.start_addr</th>
<th>From Parent Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Range End Address</td>
<td>range.end_addr</td>
<td>From Parent Range</td>
</tr>
</tbody>
</table>

**Enriched from Parent Network**

<table>
<thead>
<tr>
<th>Source IP Network View Name</th>
<th>network.network_view</th>
<th>From Parent Network</th>
<th>Network view name in string format.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Network</td>
<td>network.network</td>
<td>From Parent Network</td>
<td>ip_addr/cidr Example: 1.2.3.4/24</td>
</tr>
<tr>
<td>Source IP Network Address</td>
<td>network.ipv4addr</td>
<td>From Parent Network</td>
<td>ip_addr</td>
</tr>
<tr>
<td>Source IP Network Cidr</td>
<td>network.netmask</td>
<td>From Parent Network</td>
<td>CIDR</td>
</tr>
</tbody>
</table>
Source IP Network EA | network.extattrs | From Parent Network EA | EA name can be any UTF-8 characters.
--- | --- | --- | ---
**Enriched from Lease Data**
Source IP Lease Start Time | lease.starts (ISO 8601 format) | From Lease Data
Source IP Lease End Time | lease.ends (ISO 8601 format) | From Lease Data
Source IP Lease State | lease.binding_state | From Lease Data
Source IP Lease Client Host Name | lease.client_hostname | From Lease Data
Source IP Lease MAC Address | lease.hardware | From Lease Data
Source IP Lease DUID | lease.ipv6_duid | From Lease Data
Source IP Fingerprint | lease.fingerprint | From Lease Data

### Table 45.15 Variables for DB Object Change Event - DHCP Network IPv4

<table>
<thead>
<tr>
<th>NIOS Field Name</th>
<th>Template Variable Name</th>
<th>Filter</th>
<th>Enriched Data</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>timestamp (ISO 8601 format)</td>
<td></td>
<td></td>
<td>When the event occurs</td>
</tr>
<tr>
<td>Infoblox Member IP</td>
<td>member_ip</td>
<td></td>
<td></td>
<td>Infoblox member IP (VIP or LAN1) that has generated the event.</td>
</tr>
<tr>
<td>Infoblox Member Name</td>
<td>member_name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAPI object reference</td>
<td>_ref</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>comment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable</td>
<td>disable</td>
<td>equals</td>
<td></td>
<td>Boolean</td>
</tr>
<tr>
<td>Extensible Attributes</td>
<td>extattrs</td>
<td></td>
<td></td>
<td>dictionary of extensible attributes</td>
</tr>
<tr>
<td>Network</td>
<td>network</td>
<td>equals, contained in</td>
<td>ip_addr/cidr</td>
<td></td>
</tr>
<tr>
<td>network_view</td>
<td>network_view</td>
<td>contains, equals, begins with, ends with</td>
<td>String format</td>
<td></td>
</tr>
<tr>
<td>Members</td>
<td>members</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS AD User Data</td>
<td>ms_ad_user_data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>comment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>network_container</td>
<td>network_container</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>options</td>
<td>options</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>unmanaged</td>
<td>unmanaged</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Type</td>
<td>event_type</td>
<td>equals</td>
<td>RPZ</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>--------</td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LEASE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TUNNEL</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NETWORK_IPV4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NETWORK_IPV6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RANGE_IPV4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RANGE_IPV6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FIXED_ADDRESS_IPV4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FIXED_ADDRESS_IPV6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HOST_ADDRESS_IPV4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HOST_ADDRESS_IPV6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SESSION</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SESSION is used for the login and logout events for the session management templates.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 45.16 Variables for DB Object Change Event - DHCP Network IPv6

<table>
<thead>
<tr>
<th>NIOS Field Name</th>
<th>Template Variable Name</th>
<th>Filter</th>
<th>Enriched Data</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>timestamp (ISO 8601 format)</td>
<td></td>
<td></td>
<td>When the event occurs</td>
</tr>
<tr>
<td>Infoblox Member IP</td>
<td>member_ip</td>
<td></td>
<td></td>
<td>Infoblox member IP (VIP or LAN1) that has generated the event.</td>
</tr>
<tr>
<td>Infoblox Member Name</td>
<td>member_name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAPI object reference</td>
<td>_ref</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>comment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable</td>
<td>disable</td>
<td>equals</td>
<td></td>
<td>Boolean</td>
</tr>
<tr>
<td>Extensible Attributes</td>
<td>extattrs</td>
<td></td>
<td></td>
<td>Dictionary of extensible attributes</td>
</tr>
<tr>
<td>Network</td>
<td>network</td>
<td>equals, contained in</td>
<td>ip_addr/cidr</td>
<td></td>
</tr>
<tr>
<td>network_view</td>
<td>network_view</td>
<td>contains, equals, begins with, ends with</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>Members</td>
<td>members</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS AD User Data</td>
<td>ms_ad_user_data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>comment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>network_container</td>
<td>network_container</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>options</td>
<td>options</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>unmanaged</td>
<td>unmanaged</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Type</td>
<td>event_type</td>
<td>equals</td>
<td>RPZ</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LEASE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TUNNEL</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NETWORK_IPV4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NETWORK_IPV6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RANGE_IPV4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RANGE_IPV6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FIXED_ADDRESS_IPV4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FIXED_ADDRESS_IPV6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HOST_ADDRESS_IPV4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HOST_ADDRESS_IPV6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SESSION</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SESSION is used for the login and logout events for the session management templates.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 45.17 Variables for DB Object Change Event - DHCP Range IPv4

<table>
<thead>
<tr>
<th>NIOS Field Name</th>
<th>Template Variable Name</th>
<th>Supported Filter</th>
<th>Enriched Data</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>timestamp (ISO 8601 format)</td>
<td></td>
<td></td>
<td>When the event occurs</td>
</tr>
<tr>
<td>Infoblox Member IP</td>
<td>member_ip</td>
<td></td>
<td></td>
<td>Infoblox Member IP (VIP or LAN1) that has generated the event.</td>
</tr>
<tr>
<td>WAPI object reference</td>
<td>_ref</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>comment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable</td>
<td>disable</td>
<td>equals</td>
<td></td>
<td>Boolean</td>
</tr>
<tr>
<td>Extensible Attributes</td>
<td>extattrs</td>
<td></td>
<td></td>
<td>Dictionary of extensible attributes</td>
</tr>
<tr>
<td>Network</td>
<td>network</td>
<td>equals, contained in</td>
<td></td>
<td>ip_addr/cidr</td>
</tr>
<tr>
<td>network_view</td>
<td>network_view</td>
<td>contains, equals, begins with, ends with</td>
<td></td>
<td>String</td>
</tr>
<tr>
<td>Member</td>
<td>member</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boot File</td>
<td>bootfile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start Address</td>
<td>start_addr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End Address</td>
<td>end_addr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Filter Rules</td>
<td>mac_filter_rules</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS AD User Data</td>
<td>ms_ad_user_data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Next Server</td>
<td>nextserver</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Association Type</td>
<td>server_association_type</td>
<td>contains, equals, begins with, ends with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Type</td>
<td>event_type</td>
<td>equals</td>
<td></td>
<td>RPZ&lt;br&gt;LEASE&lt;br&gt;TUNNEL&lt;br&gt;NETWORK_IPV4&lt;br&gt;NETWORK_IPV6&lt;br&gt;RANGE_IPV4&lt;br&gt;RANGE_IPV6&lt;br&gt;FIXED_ADDRESS_IPV4&lt;br&gt;FIXED_ADDRESS_IPV6&lt;br&gt;HOST_ADDRESS_IPV4&lt;br&gt;HOST_ADDRESS_IPV6&lt;br&gt;SESSION</td>
</tr>
</tbody>
</table>

### Table 45.18 Variables for DB Object Change Event - DHCP Range IPv6

<table>
<thead>
<tr>
<th>NIOS Field Name</th>
<th>Template Variable Name</th>
<th>Supported Filter</th>
<th>Enriched Data</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>timestamp (ISO 8601 format)</td>
<td></td>
<td></td>
<td>Timestamp when the event occurs.</td>
</tr>
<tr>
<td>Infoblox Member IP</td>
<td>member_ip</td>
<td></td>
<td></td>
<td>Infoblox Member IP (VIP or LAN1) that has generated the event.</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infoblox Member Name</td>
<td>member_name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAPI object reference</td>
<td>_ref</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>comment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable</td>
<td>disable</td>
<td>equals Boolean</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extensible Attributes</td>
<td>extattrs</td>
<td>Dictionary of extensible attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>network</td>
<td>equals, contained in ip_addr/cidr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>network_view</td>
<td>network_view</td>
<td>contains, equals, begins with, ends with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member</td>
<td>member</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boot File</td>
<td>bootfile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start Address</td>
<td>start_addr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End Address</td>
<td>end_addr</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Filter Rules</td>
<td>mac_filter_rules</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS AD User Data</td>
<td>ms_ad_user_data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Next Server</td>
<td>nextserver</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Association Type</td>
<td>server_association_type</td>
<td>contains, equals, begins with, ends with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Type</td>
<td>event_type</td>
<td>equals</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RPZ, LEASE, TUNNEL, NETWORK_IPV4, NETWORK_IPV6, RANGE_IPV4, RANGE_IPV6, FIXED_ADDRESS_IPV4, FIXED_ADDRESS_IPV6, HOST_ADDRESS_IPV6, HOST_ADDRESS_IPV6, SESSION</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SESSION is used for the login and logout events for the session management templates.

Table 45.19 Variables for DB Object Change Event - DHCP Fixed Address IPv4

<table>
<thead>
<tr>
<th>NIOS Field Name</th>
<th>Template Variable Name</th>
<th>Supported Filter</th>
<th>Enriched Data</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>timestamp (ISO 8601 format)</td>
<td></td>
<td></td>
<td>The timestamp when the event occurs.</td>
</tr>
<tr>
<td>Infoblox Member IP</td>
<td>member_ip</td>
<td></td>
<td></td>
<td>Infoblox member IP (VIP or LAN1) that has generated the event.</td>
</tr>
<tr>
<td>Infoblox Member Name</td>
<td>member_name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAPI object reference</td>
<td>_ref</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>comment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable</td>
<td>disable</td>
<td>equals</td>
<td></td>
<td>Boolean</td>
</tr>
<tr>
<td>Extensible Attributes</td>
<td>extattrs</td>
<td></td>
<td></td>
<td>Dictionary of extensible attributes</td>
</tr>
<tr>
<td>Field</td>
<td>Variable Name</td>
<td>Supported Filter</td>
<td>Enriched Data</td>
<td>Comment</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------</td>
<td>-------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network</td>
<td>network</td>
<td>equals, contained in</td>
<td>ip_addr/cidr</td>
<td></td>
</tr>
<tr>
<td>network_view</td>
<td>network_view</td>
<td>contains, equals, begins with, ends with</td>
<td>String format</td>
<td></td>
</tr>
<tr>
<td>MS AD User Data</td>
<td>ms_ad_user_data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>name</td>
<td>contains, equals, begins with, ends with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>mac</td>
<td>contains, equals, begins with, ends with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>ipv4addr</td>
<td>equals, matches range, matches CIDR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Type</td>
<td>event_type</td>
<td>equals</td>
<td>RPZ, LEASE, TUNNEL, NETWORK_IPV4, NETWORK_IPV6, RANGE_IPV4, RANGE_IPV6, FIXED_ADDRESS_IPV4, FIXED_ADDRESS_IPV6, HOST_ADDRESS_IPV4, HOST_ADDRESS_IPV6, SESSION</td>
<td>SESSION is used for the login and logout events for the session management templates.</td>
</tr>
</tbody>
</table>

Table 45.20 Variables for DB Object Change Event - DHCP Fixed Address IPv6

<table>
<thead>
<tr>
<th>NIOS Field Name</th>
<th>Template Variable Name</th>
<th>Supported Filter</th>
<th>Enriched Data</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>timestamp (ISO 8601 format)</td>
<td></td>
<td></td>
<td>The timestamp when the event occurs.</td>
</tr>
<tr>
<td>Infoblox Member IP</td>
<td>member_ip</td>
<td></td>
<td></td>
<td>Infoblox member IP (VIP or LAN1) that has generated the event.</td>
</tr>
<tr>
<td>Infoblox Member Name</td>
<td>member_name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAPI object reference</td>
<td>_ref</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>comment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable</td>
<td>disable</td>
<td>equals</td>
<td></td>
<td>Boolean</td>
</tr>
<tr>
<td>Extensible Attributes</td>
<td>extattrs</td>
<td></td>
<td></td>
<td>Dictionary of extensible attributes</td>
</tr>
<tr>
<td>Network</td>
<td>network</td>
<td>equals, contained in</td>
<td></td>
<td>ip_addr/cidr</td>
</tr>
<tr>
<td>network_view</td>
<td>network_view</td>
<td>contains, equals, begins with, ends with</td>
<td>String format</td>
<td></td>
</tr>
<tr>
<td>MS AD User Data</td>
<td>ms_ad_user_data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>name</td>
<td>contains, equals, begins with, ends with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 DUID</td>
<td>duid</td>
<td>contains, equals, begins with, ends with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address Type</td>
<td>address_type</td>
<td>equals</td>
<td></td>
<td>Address, Prefix, or Both</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>ipv6addr</td>
<td>equals, matches range, matches CIDR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Address Prefix</td>
<td>ipv6prefix</td>
<td>equals, matches range, matches CIDR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Address Prefix bits</td>
<td>ipv6prefix_bits</td>
<td>equals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Type</td>
<td>event_type</td>
<td>equals, matches range, matches CIDR</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 45.21 Variables for DB Object Change Event - DHCP Host Address IPv4**

<table>
<thead>
<tr>
<th>NIOS Field Name</th>
<th>Template Variable Name</th>
<th>Supported Filter</th>
<th>Enriched Data</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>timestamp</td>
<td>(ISO 8601 format)</td>
<td></td>
<td>The timestamp when the event occurs.</td>
</tr>
<tr>
<td>Infoblox Member IP</td>
<td>member_ip</td>
<td></td>
<td></td>
<td>Infoblox member IP (VIP or LAN1) that has generated the event.</td>
</tr>
<tr>
<td>Infoblox Member Name</td>
<td>member_name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAPI object reference</td>
<td>_ref</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extensible Attributes</td>
<td>extattrs</td>
<td></td>
<td></td>
<td>Dictionary of extensible attributes from parent host record</td>
</tr>
<tr>
<td>Network</td>
<td>network</td>
<td>equals, contained in</td>
<td>ip_addr/cidr</td>
<td></td>
</tr>
<tr>
<td>network_view</td>
<td>network_view</td>
<td>contains, equals, begins with, ends with</td>
<td>String format</td>
<td></td>
</tr>
<tr>
<td>MS AD User Data</td>
<td>ms_ad_user_data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host</td>
<td>host</td>
<td>contains, equals, begins with, ends with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>mac</td>
<td>contains, equals, begins with, ends with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>ipv4addr</td>
<td>equals, matches range, matches CIDR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Type</td>
<td>event_type</td>
<td>equals</td>
<td>RPZ LEASE TUNNEL NETWORK_IPV4 NETWORK_IPV6 RANGE_IPV4 RANGE_IPV6 FIXED_ADDRESS_IPV4 FIXED_ADDRESS_IPV6 HOST_ADDRESS_IPV4 HOST_ADDRESS_IPV6 SESSION</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>--------</td>
<td>--------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>

SESSION is used for the login and logout events for the session management templates.

| **Table 45.22 Variables for DB Object Change Event - DHCP Host Address IPv6** |
|---------------------------------|-----------------|----------------|--------|-----------------------------|
| **NIOS Field Name** | **Template Variable Name** | **Supported Filter** | **Enriched Data** | **Comment** |
| Timestamp | timestamp (ISO 8601 format) |  |  | The timestamp when the event occurs. |
| Infoblox Member IP | member_ip |  |  | Infoblox member IP (VIP or LAN1) that has generated the event. |
| Infoblox Member Name | member_name |  |  |  |
| WAPI object reference | _ref |  |  |  |
| Extensible Attributes | extattrs |  |  | Dictionary of extensible attributes from parent host record |
| Network | network | equals, contained in | ip_addr/cidr |  |
| network_view | network_view | contains, equals, begins with, ends with | String format |  |
| MS AD User Data | ms_ad_user_data | contains, equals, begins with, ends with |  |  |
| Host | host | contains, equals, begins with, ends with |  |  |
| IPv6 DUID | duid | contains, equals, begins with, ends with |  |  |
| Address Type | address_type | equals |  |  |
| IPv6 Address | ipv6addr | equals, matches range, matches CIDR |  |  |
| IPv6 Address Prefix | ipv6prefix | equals, matches range, matches CIDR |  |  |
| IPv6 Address Prefix bits | ipv6prefix_bits | equals |  |  |
Result Parsing

Besides the R: name space, which is always initialized, if a template step includes the parse setting, then the result returned by the server is interpreted and will be available in the P: name space. Result parsing is extremely naive and supports only the following:

- **JSON**: In this case, the returned JSON will be available in the P name space if it is a dictionary, otherwise it will be as-is in the P:PARSE variable. If JSON is malformed, an error will be logged and P:PARSE will be set to an empty dictionary.

- **REGEX**: The supplied REGEX is applied to the whole body and it will be available in P:PARSE[0] to P:PARSE[N], if you have specified more than one groupings. In this case, P:PARSE[0] contains the full match, and P:PARSE[1..N] contains each individual grouping match. If no groupings are parsed, then P:PARSE will be a string with the matched expression. If one grouping is parsed, then P:PARSE will be a string with the matched grouping result. Note that ^ and $ anchors are the anchors for the whole output to be parsed.

- **RESEXLINE**: The supplied REGEX is applied to every line returned by the server, and each match is assigned to P:PARSE[0] to P:PARSE[N] depending on how many lines match. The REGEX must contain only one grouping. If there are many groupings then the last matched grouping is put in the PARSE value, but if there are no groupings provided then the full match is put in each line. Note that ^ and $ anchors in this case are the anchors for each line.

- **RESEXMULTILINE**: REGEXMULTILINE can be used when multiple groupings are required to be matched in multiple lines. Each match will be in P:PARSE[0..n] and each individual match is a list where the first value is the full REGEX match, and each subsequent value is a grouping match. The first grouping match of the first match can be accessed via ${P:PARSE[0][1]}. Note that ^ and $ anchors in this case are the anchors for each line.

For all REGEX cases, if there are no matches, P:PARSE is set to an empty string.

- **CONDITION**: In some cases, when a condition on a REGEX match is required, it is recommended to use a CONDITION step with the :L (length) format specifier applied to PARSE. So when ${P:L:PARSE} is matched with = 0, it would create a condition evaluating to true if there was a regular expression match.

- **XML**: For XML, the XML data is converted into a dictionary of dictionaries/lists depending on the XML present. Similar to JSON, this will be available in the P name space if it is a dictionary, otherwise it will be as-is in the P:PARSE variable. If the XML is malformed or not parseable, then an error is logged and P:PARSE is set to an empty dictionary.

Parsing does not support DTDs, schemas, or XML attributes. It simply converts the XML document as-is. This also means that if the schema defines a particular element to be a list, it might not be deserialized as a list depending on how many members are present (if there is only one, then the parent is not considered a list.) When serializing XML, any variable composed of a dictionary with an '<xmla>' member set to True will be serialized as an XML element with attributes.

If an XMLA element is serialized under JSON/XML, the attributes will be ignored and the appliance returns a meaningful result (a list of XMLA variables will be serialized in JSON as a list of the values of these elements, assuming the values are simple strings/numbers).

For example, consider the following XML:

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE APPLIANCE_LIST_OUTPUT SYSTEM
  "https://qualysapi.qualys.com/api/2.0/fo/appliance/appliance_list_output.dtd">
<APPLIANCE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2014-01-02T09:26:01Z</DATETIME>
    <APPLIANCE_LIST>
      <APPLIANCE>
        <ID>777</ID>
        <NAME>scanner1</NAME>
      </APPLIANCE>
    </APPLIANCE_LIST>
  </RESPONSE>
</APPLIANCE_LIST_OUTPUT>
```
The XML will be deserialized as follows:

```json
{
    "APPLIANCE_LIST_OUTPUT": {
        "RESPONSE": {
            "APPLIANCE_LIST": [
                {
                    "ID": "777",
                    "NAME": "scanner1",
                    "RUNNING_SCAN_COUNT": "0",
                    "S2": "Online",
                    "SOFTWARE_VERSION": "2.6",
                    "STATUS": "Online"
                },
                {
                    "ID": "1127",
                    "NAME": "scanner2",
                    "RUNNING_SCAN_COUNT": "0",
                    "S2": "Online",
                    "SOFTWARE_VERSION": "2.6",
                    "STATUS": "Online"
                },
                {
                    "ID": "1131",
                    "NAME": "scanner3",
                    "RUNNING_SCAN_COUNT": "0",
                    "S2": "Offline",
                    "SOFTWARE_VERSION": "2.6",
                    "STATUS": "Offline"
                }
            ]
        }
    }
}
```
"RUNNING_SCAN_COUNT": "0",
"S2": "Online",
"SOFTWARE_VERSION": "2.6",
"STATUS": "Offline"
},

"DATETIME": "2014-01-02T09:26:01Z",
"LICENSE_INFO": {
    "QVSA_LICENSES_COUNT": "10",
    "QVSA_LICENSES_USED": "3"
}
},

But the following will be deserialized differently:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE APPLIANCE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/appliance/appliance_list_output.dtd">
<APPLIANCE_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2014-01-02T09:26:01Z</DATETIME>
        <APPLIANCE_LIST>
            <APPLIANCE>
                <ID>777</ID>
                <NAME>scanner1</NAME>
                <SOFTWARE_VERSION>2.6</SOFTWARE_VERSION>
                <RUNNING_SCAN_COUNT>0</RUNNING_SCAN_COUNT>
                <STATUS>Online</STATUS>
            </APPLIANCE>
        </APPLIANCE_LIST>
        
    </RESPONSE>
</APPLIANCE_LIST_OUTPUT>
```

The XML will be deserialized as follows (note the difference in the appliance_list):

```json
{
    "APPLIANCE_LIST_OUTPUT": {
        "RESPONSE": {
            "APPLIANCE_LIST": {
                "APPLIANCE": {
                    "ID": "777",
                    "NAME": "scanner1",
                    "SOFTWARE_VERSION": "2.6",
                    "RUNNING_SCAN_COUNT": "0",
                    "STATUS": "Online"
                }
            }
        }
    }
}
```
XMLA: Infoblox strongly recommends that you use XMLA as the quoting option (as opposed to XML) when you create new action templates. New operations such as PUSH, POP, SHIFT and others are not officially supported for XML parsed data.

XMLA parsing strips all white spaces (horizontal tab, line feed, vertical tab, form feed, carriage return, and space). To keep all white spaces, XMLA_WHITESPACE enum is added. The parsing is the same as XMLA except that there is no white space stripping.

If you set parse to XMLA, the XML parsing supports XML attributes, and the XML document is put in the P:PARSE namespace variable, as illustrated in the following example. This example contains a mixed-attribute XML message with some values that contain attributes and some do not.

```xml
<?xml version="1.0" encoding="utf-8"?>
<SiteConfigResponse success="1">
    <Site id="27" name="SOAPUI13006925d-7dac-428d-aaf1-4038a98838a1" description="" riskfactor="1.0" isDynamic="0">
        <Description/>
        <Hosts a0="123">
            <host a1="123">server1.example.com</host>
            <host>server2.example.com</host>
            <host>server3.example.com</host>
            <host>server4.example.com</host>
            <host>server5.example.com</host>
        </Hosts>
        <Credentials/>
        <Alerting>
            <Alert name="test" enabled="1" maxAlerts="2">
                <scanFilter scanStart="1" scanStop="1" scanFailed="1" scanResumed="1" scanPaused="1"/>
                <vulnFilter severityThreshold="1" confirmed="1" unconfirmed="1" potential="1"/>
                <smtpAlert sender="user1@example.com" server="server6.example.com" limitText="0">
                    <recipient>user2@example.com</recipient>
                </smtpAlert>
            </Alert>
        </Alerting>
        <Schedules></Schedules>
    </Site>
</SiteConfigResponse>
```

The following is the deserialized response in P:PARSE when using XMLA parsing:

```json
[
  {
    "NAME": "scanner1",
    "RUNNING_SCAN_COUNT": "0",
    "S2": "Online",
    "SOFTWARE_VERSION": "2.6",
    "STATUS": "Online"
  },
  {
    "DATETIME": "2014-01-02T09:26:01Z",
    "LICENSE_INFO": {
      "QVSA_LICENSES_COUNT": "10",
      "QVSA_LICENSES_USED": "3"
    }
  }
]```
"<xmla>": true,
"attrs": {
   "success": "1"
},
"index": {
   "Site": 0
},
"name": "SiteConfigResponse",
"value": []
}
"<xmla>": true,
"attrs": {
   "description": "",
   "id": "27",
   "isDynamic": "0",
   "name": "SOAPUI13006925d-7dac-428d-aaf1-4038a98838a1",
   "riskfactor": "1.0"
},
"index": {
   "Alerting": 3,
   "Credentials": 2,
   "Description": 0,
   "Hosts": 1,
   "ScanConfig": 4
},
"name": "Site",
"value": [
{ "<xmla>": true,
   "attrs": {},
   "index": {},
   "name": "Description",
   "value": []
},
{ "<xmla>": true,
   "attrs": {
      "a0": "123"
   },
   "index": {
      "host": 4
   },
   "name": "Hosts",
   "value": [
    { "<xmla>": true,
      "attrs": {
         "a1": "123"
      },
      "index": {},
      "name": "host",
      "value": ["server1.example.com"]
    },
    { "<xmla>": true,
      "attrs": {},
      "index": {},
      "name": "host",
      "value": ["server2.example.com"]
   ]
}
"<xmla": true,
"attrs": {},
"index": {},
"name": "host",
"value": ["server3.example.com"]
},
"<xmla": true,
"attrs": {},
"index": {},
"name": "host",
"value": ["server4.example.com"]
},
"<xmla": true,
"attrs": {},
"index": {},
"name": "host",
"value": ["server5.example.com"]
}]
},
"<xmla": true,
"attrs": {},
"index": {}
"name": "Credentials",
"value": []
},
"<xmla": true,
"attrs": {},
"index": { "Alert": 0 }
},
"name": "Alerting",
"value": [
{ "<xmla": true,
"attrs": { 
"enabled": "1",
"maxAlerts": "2",
"name": "test"
 },
"index": { 
 "scanFilter": 0,
 "smtpAlert": 2,
 "vulnFilter": 1
 },
 "name": "Alert",
 "value": [ 
 { "<xmla": true,
 "attrs": { 
 "scanFailed": "1",
 "scanPaused": "1",
 "scanResumed": "1",
 "scanStart": "1",
 "scanStop": "1"
 },
 "index": {},
 "name": "scanFilter",
 "value": []
 },
As shown in the example above, any XML value will become an internal dictionary that contains separate 'attrs' and 'value' members representing the XML attributes (if exist) and the XML values (if exist) of the element respectively, as well as the single "" boolean (set to True) to qualify this particular field as an XML attribute field (this is used when serializing, as well as for user-created XMLA values, see below).

You typically address the XMLA variable by using \( \text{VAR\{tag\{subtag\}} \), which uses the VALUES of the tag (its value or its subtag(s)). To access the attributes of a tag, you use \( \text{VAR\{tag\{attributename\}} \). Example: \( \text{P::PARSE\{SiteConfigResponse\}} \{\{success\}\} \)

If you need to access the name of a tag instead (for example if the remote server can return different tags depending on the status), use the \( \text{[[name]]} \) syntax. For example, you can use \( \text{P::PARSE\{[name]\}} \).

**Adding Outbound Templates**

Before you configure notification rules, you must add or upload outbound templates to the Grid. The appliance uses the scripts in these templates to process and sends outbound notifications to the endpoints. You can either modify existing templates or create new ones through Grid Manager. For information about how to create a template, see [Creating Action Templates](#).

**Note:** When you add an outbound template or make changes to an existing one, it may take a few seconds to a few minutes until the changes are propagated to all the members.

Complete the following to upload an outbound template:

1. From the **Grid** tab, select the **Ecosystem** tab -> **Templates** tab, and then click the Add icon.  
   or  
   From the **Grid** tab, select the **Ecosystem** tab, and click **Add Template** from the Toolbar.
2. In the **Add Template** wizard, complete the following:
   - Click **Select** to upload an outbound template. In the **Upload** dialog box, click **Select** and navigate to the template, and then click **Upload**. Select the **Overwrite the existing template** check box to overwrite an existing template.
3. Click **Add** to add an outbound template.
4. Optionally, click **ViewResults** to open the **Syslog Preview** dialog and view all the syslog messages. For more information, see [Previewing Syslog Events](#).

**Modifying Outbound Templates**

To modify an outbound template:

1. From the **Grid** tab, select the **Ecosystem** tab -> **Templates** tab -> **template** check box, and then click the Edit icon.  
   or  
   From the **Grid** tab, select the **Ecosystem** tab, select the template that you want to modify, click the Action icon and select **Edit**.
2. The `<Template Name>`**Template** editor contains the following tabs from which you can modify information:
   - **General:** You can modify the **Name** and **Comment** fields. All other fields are automatically propagated with available information, such as the template type, vendor type, event type, and action type.
   - **Contents:** This tab displays the content of the uploaded template file. You can modify the template contents and the appliance validates the content for proper JSON format when you save the configuration. For more information about the format of the templates, see [Creating Session Management Templates](#) and [Creating Action Templates](#).
3. Save the configuration.

**Viewing All Outbound Templates**

To view the list of outbound templates:
1. From the Grid tab, select the Ecosystem tab, and then click the Templates tab.

2. Grid Manager displays the following information:
   - **Name**: The outbound template name.
   - **Vendor Type**: The vendor type.
   - **Event Type**: The event type specified in the template.
   - **Template Type**: Displays the template type, such as Session Management or Action template.
   - **Outbound Type**: The endpoint type. This can be REST or DXL.
   - **Comment**: Comments that were entered for the outbound template.
   - **Added On**: Displays the timestamp when the template was uploaded to the Grid Master in this format: YYYY-MM-DD HH:MM:SS, plus time zone.

You can do the following in this tab:

- You can select the Action icon

  ![Action Icon](image)

  and do the following:
  - **Edit**: Select this to modify the outbound template information.
  - **Delete**: Select this to delete a template.
  - **Export**: Select this to export a template.

- Edit the outbound template information.
  - Select the outbound template, and then click the Edit icon.

- Delete an outbound template.
  - Select the template, and then click the Delete icon.

- Export the list of outbound templates.
  - Click the Export icon.

- Print the list of outbound templates.
  - Click the Print icon.

- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.

- Create a quick filter to save frequently used filter criteria:
  
  a. In the filter section, click **Show Filter** and define filter criteria for the quick filter.
  b. Click **Save** and complete the configuration in the Save Quick Filter dialog box.

  The appliance adds the quick filter to the quick filter drop-down list in the panel. Note that global filters are prefixed with [G], local filters with [L], and system filters with [S].

- Sort the outbound templates in ascending or descending order by column.

### Deleting Outbound Templates

You can delete a template anytime after you have created it.

**Note**: Before you delete a template, ensure that it is not in use.

To delete a template:

1. From the Grid tab, select the Ecosystem tab, and then click the Templates tab.
2. Select the template that you want to delete, and click the Delete icon.
3. Click **Yes** in the Delete Confirmation dialog.

### Exporting Template Schema

The Export Template Schema feature allows you to export the session management and action template schema. You can use the exported schema to validate the templates before uploading them. The exported schema is in IETF JSON Schema format. It is a JSON file that is used to define and validate outbound templates you plan to upload to the appliance. If you want to create your own templates, you must follow this schema format. For information about this format, see [https://tools.ietf.org/html/draft-zyp-json-schema-04](https://tools.ietf.org/html/draft-zyp-json-schema-04).

Complete the following to export the outbound template schema:

1. From the Grid tab, select the Ecosystem tab -> select the Templates tab.
2. Expand the Toolbar, click **ExportTemplateSchema** -> select **ActionTemplateSchema** to export the action template schema or select **SessionTemplateSchema** to export the session management template schema.
3. If there is only one template version, the appliance downloads the schema to your local system. If there are multiple template versions, the appliance displays the Export Action Template Schema or Export Session Template Schema dialog. In the dialog, select the template version that you want to export. The template schema is downloaded to your local system.
Configuring Outbound Endpoints

You can configure REST API and DXL endpoints to send outbound notifications.

To configure a REST API endpoint, complete the following:

1. From the Grid tab, select the Ecosystem tab -> Outbound Endpoint tab, and click the Add icon and select REST API Endpoint.
   Or
   From the Grid tab, select the Ecosystem tab -> Outbound Endpoint tab and then click Add -> REST API Endpoint from the Toolbar.
2. In the Add REST API Endpoint wizard, complete the following:
   - URI: Specify the URL for the endpoint to which you are sending the outbound notifications. Example: https://10.36.101.14/offices.
   - Test Connection: Click this to validate the endpoint settings and test the connectivity between the Grid Master and the endpoint (this does not test the connection between the Grid Master Candidate that is assigned as the outbound member and the endpoint), Grid Manager displays a message indicating whether the connection is successful. Note that the test does not validate username, password, or certificate for the endpoint. It only tests the basic connection between the Grid Master and the endpoint.
   - Name: Specify the name used to identify the endpoint.
   - Vendor Type: The REST API vendor type associated with the endpoint. This is optional.
   - Auth Username: Enter the username of the target endpoint. The appliance ignores the Auth Username for WAPI related steps in any action templates if WAPI integration is configured. It still uses this username for other non-WAPI related steps.
   - Auth Password: Enter the user account password for the target endpoint. You can click Clear Password to clear the password and set a new one. The appliance ignores the Auth Username for WAPI related steps in any action templates if WAPI integration is configured. It still uses this password for other non-WAPI related steps.
   - Client Certificate: Click Select to upload the endpoint certificate. In the Upload dialog box, click Select to navigate to the certificate, and then click Upload.
   - WAPI Integration Username: If you have included at least one "wapi" related field in your action template, you must configure WAPI integration; otherwise the WAPI step will fail due to an authorization error. Enter the username of the admin user you want to designate for RESTful API outbound notifications. The appliance ignores the Auth Username and Auth Password for WAPI related steps in any action templates if WAPI integration is configured.
   - WAPI Integration Password: Enter the password of the admin user you have designated for RESTful API outbound notifications.
   - Server Certificate Validation: Select one of the following for server certificate validation:
     - Use CA Certificate Validation (Recommended): Select this to validate the CA certificate for the endpoint. The certificate is used to establish a secure connection to the endpoint before data transmission. Click CA Certificates to upload the trusted CA certificate of the endpoint. In the CA Certificates dialog box, click the Add icon, and then navigate to the certificate to upload it. This is the default.
     - Enable Host Validation: Select this to enable the validation of the hostname for the endpoint, in addition to the CA certificate. If you do not select this, the appliance validates only the CA certificate.
     - Do not use validation (Not recommended): Infoblox does not recommend using this for your production system. Use this for testing purposes only.
   - Member Source outbound API requests from:
     - Selected Grid Master Candidate (Recommended): Select this to use the Grid Master Candidate to process and send outbound notifications to the endpoint. If there are multiple Grid Master candidates, select a Grid Master Candidate from the drop-down list. This is the recommended choice and is selected by default because the CPU and memory required for processing and sending outbound events from the Grid Master Candidate can be offloaded or manually load balanced across multiple Grid Master Candidates if required.

Note: If your outbound member is a Grid Master Candidate and in case the Grid Master Candidate is promoted to the Grid Master, make sure that you modify the outbound member to the Grid Master on the endpoint configuration to avoid any outbound notification failures. For information, see Modifying Outbound Endpoint Configuration.

- Current Grid Master: Click this to use the Grid Master to send outbound notifications to the endpoint. When you use the Grid Master as the outbound member, ensure that it has enough CPU and memory to process all the workloads and processes, in addition to being an outbound member. Infoblox recommends that you use the Grid Master as an outbound member only for testing purposes to avoid overloading the Grid Master and to maintain optimal performance for the Grid.
- Comment: Enter additional information about the REST API endpoint.
- Disable: Select this if you want to save the configuration but do not want to use it yet. You can clear this check box when you are ready to use this configuration.

3. Click Next to set the duration of time that the endpoint waits for a response from the outbound member. Complete the following to specify session timeout value:
   - Timeout: Specify the session timeout value for the endpoint. The default value is 30 seconds.
   - Log Level: From the drop-down list, select the severity level for the events. The severity level you select here determines the type of events that are being logged. This can be Debug, Info, Warning, or Error. When you select Debug, all fields or variables used in the events that were sent to the endpoint are logged, including deduplicated events for RPZ hits. For information about deduplication, see Deduplicating RPZ Events. Note that setting this to Debug might slightly affect the performance of your production system.
   - Template: Click Select Template to select a session management template. For information, see Creating Session Management
I Templates
- **Vendor Type**: Displays the vendor information for the endpoint.
- **Action Type**: Displays Session Management or Action based on the template you select.
- **Parameters**: Displays the parameters of the template you select. You can access these values in the notification rules.

4. Click **Next** to add extensible attributes for the endpoint. For information, see About Extensible Attributes.

5. Save the configuration.

### Configuring DXL Endpoints

When adding a DXL endpoint, you must configure the DXL client and broker. You can manually configure the list of DXL brokers that are used by DXL clients in NIOS or import the broker configuration file, as described in the following steps.

To configure a DXL endpoint, complete the following:

1. From the Grid tab, select the Ecosystem tab -> OutboundEndpoint tab, and click the Add icon and select Add DXL Endpoint.

   Or

   From the Grid tab, select the Ecosystem tab -> OutboundEndpoint tab and then click Add -> Add DXL Endpoint from the Toolbar.

2. In the Add DXL Endpoint wizard, complete the following:
   - **Name**: Specify the name used to identify the endpoint.
   - **Vendor Type**: The DXL vendor type associated with the endpoint. This is optional.
   - **Client Certificate**: Click **Generate** to generate and upload both the client and CA certificates of the endpoint on NIOS. When you click **Generate**, the client certificate is automatically uploaded on NIOS and a copy of CA certificate is downloaded. Import this downloaded CA certificate to the DXL server. For information about how to import the CA certificate, refer to the McAfee documentation. If you already have the client certificate, you can upload it by clicking the Upload icon. Click **Upload** to upload the client certificate. In the Upload dialog box, click Select to navigate to the certificate, and then click Upload.
   - **CA Certificates**: Click **CACertificates** to upload the broker Certificate. Download the broker certificate from the DXL server and upload it to NIOS. In the CA Certificates dialog box, click the Add icon, and then navigate to the certificate to upload it.
   - **WAPI Integration Username**: If you have included at least one “wapi” related field in your action template, you must configure WAPI integration; otherwise, the WAPI step will fail due to an authorization error. Enter the username of the admin user you want to designate for DXL notifications.
   - **WAPI Integration Password**: Enter the password of the admin user you have designated for DXL notifications.
   - **Member Source outbound API requests from**: Select one of the following to process for sending outbound notifications:
     - **Selected GridMaster Candidate (Recommended)**: Select this to use the Grid Master Candidate to process and send outbound notifications to the endpoint. If there are multiple Grid Master candidates, select a Grid Master Candidate from the drop-down list. This is the recommended choice and is selected by default because the CPU and memory required for processing and sending outbound events from the Grid Master Candidate can be offloaded or manually load balanced across multiple Grid Master Candidates if required.
   - **Note**: If your outbound member is a Grid Master Candidate and in case the Grid Master Candidate is promoted to the Grid Master, make sure that you modify the outbound member to the Grid Master on the endpoint configuration to avoid any outbound notification failures. For information, see Modifying Outbound Endpoint Configuration.
     - **Current Grid Master**: Click this to use the Grid Master to send outbound notifications to the endpoint. When you use the Grid Master as the outbound member, ensure that it has enough CPU and memory to process all the workloads and processes, in addition to being an outbound member. Infoblox recommends that you use the Grid Master as an outbound member only for testing purposes to avoid overloading the Grid Master and to maintain optimal performance for the Grid.
     - **Comment**: Enter additional information about the DXL endpoint.
     - **Disable**: Select this if you want to save the configuration but do not want to use it yet. You can clear this check box when you are ready to use this configuration.

3. Click **Next** to add the DXL broker. There are two ways to configure the DXL broker. You can manually enter the host name of the broker or you can import the broker configuration file using the Import option. In the Brokers wizard, do one of the following:
   - **Click Add** to open the Add Broker wizard. Enter the host name in the Host Name text box. Optionally, you can enter the following information as well:
     - **IP address**: Enter the IP address of the DXL broker.
     - **Unique ID**: A unique identifier for the broker. This is useful for identifying the DXL broker in log messages.
     - **Port information**: The port number used to communicate with the DXL broker.
   - **Click Import** to upload the broker configuration file. In the Upload dialog box, click Select to navigate to the certificate, and then click Upload.

   **Note**: You can export the Broker configuration file from McAfee ePolicy Orchestrator (McAfee ePO). For information how to export, refer to the McAfee documentation.

   Click **Test Connection** to validate the connectivity between the DXL broker fabric and the Grid Master.

4. Click **Next** to set the severity level for the events.
• **Log Level**: From the drop-down list, select the severity level for the events. The severity level you select here determines the type of events that are being logged. This can be **Debug**, **Info**, **Warning**, or **Error**. When you select **Debug**, all fields or variables used in the events that were sent to the endpoint are logged, including deduplicated events for RPZ hits. For information about deduplication, see **Deduplicating RPZ Events**. Note that setting this to **Debug** might slightly affect the performance of your production system.

• **Vendor Type**: Displays the vendor information for the endpoint.

• **Template Type**: Displays Session Management.

• **Parameters**: Displays the parameters of the template you select. You can access these values in the notification rules.

5. Click **Next** to add extensible attributes for the endpoint. For information, see **About Extensible Attributes**.

6. Save the configuration.

### Modifying Outbound Endpoint Configuration

To modify an endpoint configuration:

1. From the **Grid** tab, select the **Ecosystem** tab -> **Outbound Endpoint** tab, click the **Action** icon next to the endpoint name and select **Edit** from the menu.

2. The `<Endpoint Name>` **Endpoint** editor provides the following tabs from which you can modify data:
   - **General**: You can modify the general information of an endpoint, as described in **Configuring Outbound Endpoints**.
   - **Brokers**: You can modify the DXL broker configuration, as described in **Configuring DXL Endpoints**. This tab is available only for DXL endpoints.
   - **Session Management**: You can edit the session timeout value and upload a new session management template.
   - **Extensible Attributes**: You can add, modify, and delete extensible attributes that are associated with an endpoint. For information, see **About Extensible Attributes**.

3. Save the configuration.

### Viewing All Outbound Endpoints

The **Outbound Endpoint** tab displays all outbound endpoints that are configured on the NIOS appliance.

To view the list of outbound endpoints:

1. From the **Grid** tab, select the **Ecosystem** tab, and click the **Outbound Endpoint** tab.

2. Grid Manager displays the following information for each endpoint:
   - **Name**: The name of the endpoint.
   - **Endpoint Type**: The endpoint type, such as DXL or REST API.
   - **URI**: The URL to which the outbound notifications are sent.
   - **Vendor**: The vendor type associated with the endpoint.
   - **Outbound Member**: The outbound member that processes and sends outbound notifications. This can be either the Grid Master Candidate or the Grid Master. Infoblox recommends that you select the Grid Master Candidate and this is selected by default.
   - **Comment**: Additional information about the endpoint configuration.
   - **Client Certificate Valid From**: The timestamp when the client certificate for a notification endpoint is created.
   - **Client Certificate Valid To**: The timestamp when the client certificate for a notification endpoint expires.
   - **Disabled**: Indicates whether the endpoint is disabled.
   - **Site**: This is a predefined extensible attribute.

You can also do the following in this tab:

- Click the **Action** icon

  ![Action Icon](image)

  and do the following:

  - **Edit**: Select this to modify the endpoint information.
  - **Delete**: Select this to delete an endpoint.
  - **View Debug Log**: Select this to view debug messages about all events associated with the selected endpoint. Through a separate browser, you can view the debug logs from all Grid members.

  - Edit an outbound endpoint information.
  - Select the `<REST API or DXL>` endpoint, and then click the **Edit** icon.
  - Delete an outbound endpoint.
  - Select the `<REST API or DXL>` endpoint, and then click the **Delete** icon.
  - Export the list of outbound endpoints.
  - Click the **Export** icon.
  - Print the list of outbound endpoints.
  - Click the **Print** icon.

  - Use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.

  - Create a quick filter to save frequently used filter criteria:

    - In the filter section, click **Show Filter** and define filter criteria for the quick filter.
b. Click Save and complete the configuration in the Save Quick Filter dialog box.

The appliance adds the quick filter to the quick filter drop-down list in the panel. Note that global filters are prefixed with [G], local filters with [L], and system filters with [S].

- Sort the outbound end points in ascending or descending order by column.

### Configuring Notification Rules

You can configure notification rules after you have uploaded outbound templates and configured outbound endpoints on the NIOS appliance. For information about adding outbound endpoints, see Configuring Outbound Endpoints. To send outbound notifications from NIOS to the target endpoints, you must configure notification rules. When adding rules, you must associate the correct action template to the rule. The appliance validates the event type specified in the template with the event type that you select in the notification rule. The parameters defined in a template decides the way NIOS specific data is presented to an endpoint. Each notification rule specifies the target endpoint, notification rule criteria, and the outbound template being used to take action for the matching events.

**Note:** When you remove all the notification rules associated with an endpoint, all the debug logs for that endpoint will also be removed.

While configuring notification rules, you can decide whether you want to reduce the amount of redundant RPZ hit events or not. Oftentimes, RPZ hits come from the same client IPs, query FQDNs, or networks. To avoid receiving excessive RPZ events at the endpoint, you can configure the appliance to remove or deduplicate subsequent RPZ events (after sending the first event) within a certain time period based on Source IP, Query Name, RPZ Policy, and other related fields. Depending on your configuration, the appliance sends the first RPZ event and deduplicates subsequent events that match your filtering criteria within the configured lookback interval. For more information, see Deduplicating RPZ Events.

### Adding Notification Rules

To add notification rules:

1. From the Grid tab, select the Ecosystem tab -> Notification tab, and then click the Add icon.  
   or  
   From the Grid tab, select the Ecosystem tab, and click Add Notification Rule from the Toolbar.
2. In the Add Notification wizard, complete the following:
   - **Name:** Enter the name of the notification rule.
   - **Target:** Click Select Endpoint to select the endpoint type. If there are multiple endpoints, the All Endpoints Selector dialog box is displayed, from which you can select an endpoint name, such as Cisco ISE.
   - **Target Type:** Displays the target type. You cannot change this.
   - **Comment:** Enter useful information about the notification rule.
   - **Disable:** Select this option to disable the notification rule.
3. Click Next and complete the following to configure notification rules for the selected endpoint:
   - **Event:** Depending on the licenses you have installed in the Grid, you can select the event types you want to apply to the notification rules. The outbound member collects data for the selected events based on your configuration. Note that if there is a significant amount of data or if the network bandwidth is not sufficient, the outbound member might drop some of the events. In this case, you can access the syslog to view the messages related to dropped events. In addition to basic information (such as timestamp, member IP, network, and others), data collected for some event type might include enriched data such as discovered data, parent network information, and associated extensible attributes.

**Note:** The event type you select here will affect the templates that are available when you select the RESTful API template you want to use for the outbound notifications. For example, if you select DNS RPZ as the event type, only templates configured for DNS RPZ event type are available for selection.

From the drop-down list, select the event types you want to monitor for the notification rules:

- **DNS RPZ**: Select this to collect data for RPZ events. The DNS RPZ event type is available only if you have installed the RPZ license in the Grid. When you select this event type, you can enable event deduplication in the next step so the appliance can avoid sending excessive events to the endpoint based on your configuration.
- **DNS Tunneling**: Select this to collect data for DNS tunneling events.
- **DHCP Leases**: Select this to collect data for DHCP leases. Since the same IP addresses might be used by multiple systems, the appliance matches both the IP and the MAC address or the DUID to ensure the discovered data is most likely to be correct.
- **Object Change DHCP Fixed Address IPv4 and IPv6, DB Change DHCP Network IPv4 and IPv6, DB Change DHCP Range IPv4 and IPv6, DB Change DNS Host Address IPv4 and IPv6**: Select any of these to collect data for database changes in fixed addresses, DHCP ranges, networks and DNS host addresses.
- **Action**: This field is displayed only if you have selected Cisco ISE as the endpoint (the Target field). Otherwise, this field is hidden.

In the Match the following rule section, select the filters, operators and values from the drop-down lists for the selected event type. You can use the + icon to construct nested expressions for the rule. Depending on the event type you have selected, you can select the following possible filters:
• DNS RPZ: Action Policy, RPZ Name, RPZ Type, Rule Name, and Source IP
• DNS Tunneling: Source IP
• DHCP Leases: DHCP Fingerprint and Lease State.
• Object Change DHCP Fixed Address IPv4: Disable, IPv4 Address, MAC, Name, Network, and Network View
• Object Change DHCP Fixed Address IPv6: Address Type, Disable, DUID, IPv6 Address, IPv6 Prefix, IPv6 Prefix Bits, Name, Network, and Network View
• DB Change DHCP Network IPv4: Disable, Network, and Network View
• Object Change DHCP Network IPv6: Disable, Network, and Network View
• Object Change DHCP Range IPv4: Disable, Network, Network View, and Server Association Type
• Object Change DHCP Range IPv6: Address Type, Disable, Network, Network View, and Server Association Type
• Object Change DNS Host Address IPv4: Host, IPv4 Address, MAC, Network, and Network View Association Type
• Object Change DNS Host Address IPv6: Address Type, DUID, Host, IPv6 Address, IPv6 Prefix, IPv6 Prefix Bits, and Network View

4. Click Next. If you have selected DNS RPZ as the event type, go to Deduplicating RPZ Events to configure deduplication. Otherwise, go to Selecting Action Template to select an action template.

Deduplicating RPZ Events

1. This step appears only if you have selected DNS RPZ as the event type. To avoid excessive notifications received at the endpoint, complete the following to configure event deduplication:
   • Enable RPZ event deduplication: Select this to enable event deduplication for RPZ hits. When you enable deduplication, the appliance suppress redundant notifications based on your configuration.
   • Log all dropped events due to deduplication to the syslog: Select this if you want to log all the events that have been dropped due to deduplication. Selecting this allows the appliance to record all the dropped events to the syslog.
   • Select the fields to use for deduplication: From the Available table, pick the fields you want to use for filtering the deduplication and move them to the Selected table using the right arrow. You can also deselect any fields by selecting and moving them from the Selected table to the Available table using the left arrow. Event deduplication is done based on the conditions of the selected fields. The following example explains how deduplication works if two RPZ hits occur within the lookback interval, as follows:

   RPZ hit 1: source_ip: 1.2.3.4, query_name: server1.bad.com, rpz_policy: NXDOMAIN, query_type: qname, network.network_view: internal, network.network: 1.2.3.0/24
   RPZ hit 2: source_ip: 1.2.3.4, query_name: www.something.com, rpz_policy: NXDOMAIN, query_type: qname, network.network_view: internal, network.network: 1.2.3.0/24

   If you have selected only Source IP for deduplication, the appliance sends only the first RPZ event to the endpoint. If you have selected both Source IP and Query Name, both PRZ events are sent to the endpoint.

   • Lookback Interval: Enter the time interval during which the appliance evaluates RPZ hit events and stops sending redundant events to the endpoint (based on your configuration). At the end of this interval, the appliance resumes scanning of the client IP, query FQDN, or network for RPZ events. The minimum interval is five seconds and the maximum is 15 minutes. The default is 10 minutes.

2. Click Next to select an action template for the endpoint, as described in Selecting Action Template.

Selecting Action Template

1. In this step, select the outbound template you want to use for outbound notifications. The appliance validates the event type that is added to the notification rule and then matches that with the event type configured in the template.
   In the Template field, click Select Template to associate an action template with the notification rule. If there are multiple templates, the <DXL or RESTful API> Template Selector dialog box is displayed, from which you can select an action template. Note that only templates that have the same event type configured for the notification rule appear in this dialog.
   The following information is displayed about the selected action template:
   • Vendor Type: The vendor type associated with the endpoint.
   • Action Type: The type of action that will be taken for the matching events.
   • Parameters: Displays the associated parameters of the template, such as Name, Value, and Type. You can click the Value cell and modify the value for the parameter.

2. Save the endpoint configuration.

Modifying Notification Rules

To modify a notification rule:

1. From the Grid tab, select the Ecosystem tab -> Notification tab, click the Action icon next to the notification rule and select Edit from the menu.
2. The Notification Rule editor provides the following tabs from which you can modify data:
   • General: You can modify the Target and Comment fields.
**Rules:** You can edit the event type and the rule, as described in [Configuring Notification Rules](#).

**Templates:** You can select a new action template for the notification rule.

3. Save the configuration.

### Viewing All Notification Rules

To view the list of notification rules:

1. From the Grid tab, select the Ecosystem tab, and click the Notification tab.
2. Grid Manager displays the following information:
   - **Name:** Name of the notification rule.
   - **Target:** The target name.
   - **Action:** The action type.
   - **Comment:** Comments that were entered for the notification rule.
   - **Disable:** Displays whether the notification rule is disabled.

You can do the following in this tab:

- Click the Action icon

  and do the following:
  - **Edit:** Select this to modify the notification rule.
  - **Delete:** Select this to delete a notification rule.
  - **Test Rule:** Select this to execute the parameters and fields of a template against the notification criteria and verify whether the notification rule works for the event (specified in the template). Make changes to the template if required, and you can view this information in the debug log.
  - **View Debug Log:** Select this to view debugging messages for the selected notification rule.

- **Edit the notification rule information.**
  - Select the notification rule, and then click the Edit icon.
- **Delete a notification rule.**
  - Select the notification rule, and then click the Delete icon.

**Note:** When you remove all the notification rules associated with an endpoint, all the debug logs for that endpoint will also be removed.

- Print the list of notification rules.
  - Click the Print icon.
- Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria:
  
  a. In the filter section, click Show Filter and define filter criteria for the quick filter.
  b. Click Save and complete the configuration in the Save Quick Filter dialog box.

The appliance adds the quick filter to the quick filter drop-down list in the panel. Note that global filters are prefixed with [G], local filters with [L], and system filters with [S].

- Sort the notification rules in ascending or descending order by column.

### Sample Templates

This section contains sample templates that illustrate the following:

- Session management using login and logout templates
- Viewing event types
- XML parsing and handling
- Steps execution through backtracking and loops in a template
- Operations using namespace variables
- IP-related XC operations
- WAPI integration

**Note:** Some of the templates are specific for Rapid7 servers.

### Session Management Template

Following is a sample session management template for REST API endpoint:
Note: The login_template and logout_template lines specify the templates to be executed for login and logout. The session_duration line specifies the length of the session. You must upload the login and logout templates before configuring a session management template that refers them.

Following is a sample session management template for DXL endpoint:

```json
{
    "name": "session_template",
    "version": "3.0",
    "type": "DXL_ENDPOINT",
    "vendor_identifier": "DXL",
    "dxl_keep_alive_interval": 60,
    "dxl_topic": "/outbound/session"
}
```

Login Template

```json
{
    "name": "login",
    "version": "2.0",
    "vendor_identifier": "Rapid7",
    "type": "REST_EVENT",
    "event_type": ["SESSION"],
    "content_type": "text/xml",
    "quoting": "XMLA",
    "steps": [
        {
            "body": "${XC:ASSIGN:{H:Authorization}:{S:}}",
            "operation": "NOP",
            "name": "login: clear basic auth"
        },
        {
            "parse": "XMLA",
            "operation": "POST",
            "no_connection_debug": false,
        }
    ]
}
```
"name": "login: request",
"body_list": [
    "<?xml version="1.0" encoding="UTF-8"?>",
    "<LoginRequest user-id="${UT::USERNAME}" password="${UT::PASSWORD}"/>
]
],
{
    "operation": "CONDITION",
    "name": "login: errorcheck",
    "condition": {
        "statements": [],
        "condition_type": "OR",
        "else_eval": "${XC:COPY:{S:SESSID}:{P:PARSE{{session-id}}}}",
        "error": true
    }
}
}

Note: The else_eval line copies the session-id from the parsed reply (if successful); otherwise, it returns an error.

Logout Template

{
    "name": "logout",
    "version": "2.0",
    "type": "REST_EVENT",
    "vendor_identifier": "Rapid7",
    "event_type": ["SESSION"],
    "content_type": "text/xml",
    "quoting": "XMLA",
}
"steps": [
  {
    "parse": "XMLA",
    "operation": "POST",
    "no_connection_debug": false,
    "name": "logout: request",
    "body_list": [
      "<?xml version="1.0" encoding="UTF-8"?>",
      "<LogoutRequest session-id="${S::SESSID}"/>"
    ]
  },
  {
    "operation": "CONDITION",
    "name": "logout: errorcheck",
    "condition": {
      "statements": [
        {
          "op": "!=",
          "right": "${P:A:PARSE[[name]]}",
          "left": "LogoutResponse"
        },
        {
          "op": "!=",
          "right": "1",
          "left": "${P:A:PARSE[[success]]}"  
        }
      ],
      "condition_type": "OR",
      "error": true
    }
  }
]

Action Template

Following is a sample action template for DXL endpoint:

{
  "vendor_identifier": "DXL",
  "version": "3.0",
  "name": "action",
  "type": "DXL_EVENT",
}


```json
"event_type": [ "FIXED_ADDRESS_IPV4" ],
"dxl_topic": "/outbound/action",
"steps": [ 
  { 
    "operation": "DXL_SEND_EVENT",
    "name": "send_ip",
    "body": "address ${E:A:values{ipv4addr}}",
    "dxl_topic": "/outbound/step"
  }
]
}
```

Following is a sample action template for REST API endpoint:

```json
{
  "name": "action",
  "vendor_identifier": "Rapid7",
  "version": "2.0",
  "content_type": "text/xml",
  "action_type": "add network or remove IP",
  "quoting": "XMLA",
  "type": "REST_EVENT",
  "event_type": [ "FIXED_ADDRESS_IPV4", "FIXED_ADDRESS_IPV6" ],
  "steps": [ 
    { 
      "name": "check operation type",
      "operation": "CONDITION",
      "condition": { 
        "statements": [ 
          { 
            "op": "!=",
            "right": "${E:A:operation_type}",
            "left": "INSERT"
          },
          { 
            "op": "!=",
            "right": "${E:A:operation_type}",
            "left": "DELETE"
          }
        ],
        "condition_type": "AND",
        "stop": true
      }
    }
  ]
}
```
{  
  "name": "send SiteListingRequest",
  "operation": "POST",
  "body_list": [
    "<?xml version="1.0" encoding="UTF-8"?>",
    "<SiteListingRequest session-id="${S::SESSID}" />
  ],
  "parse": "XMLA"
},

{  
  "operation": "CONDITION",
  "name": "send SiteListingRequest (error check)",
  "condition": {
    "statements": [
      {
        "op": "!=",
        "right": "${P:A:PARSE[[name]]}",
        "left": "SiteListingResponse"
      },
      {
        "op": "!=",
        "right": "1",
        "left": "${P:A:PARSE{{success}}}"
      }
    ],
    "condition_type": "OR",
    "error": true,
    "else_eval": "${XC:COPY:{L:site_list}:{P:PARSE}"
  }
},

{  
  "operation": "CONDITION",
  "name": "check whether site list is empty",
  "condition": {
    "statements": [{
      "op": "==",
      "right": "${L:L:site_list}",
      "left": "0"
    }],
    "condition_type": "AND",
    "error": false,
    "else_eval": "${XC:COPY:{L:site_list}:${P:PARSE}"
  }  
}
"stop": true
}

{
  "operation": "VARIABLEOP",
  "name": "get the next site",
  "variable_ops": [
  {
    "operation": "POP",
    "type": "COMPOSITE",
    "destination": "L:a_site",
    "source": "L:site_list"
  }
  ],
  "operation": "CONDITION",
  "name": "check site name",
  "condition": {
    "statements": [
      {
        "op": "!=",
        "right": "${L:A:a_site{{name}}}",
        "left": "${E:A:values{extattrs}{r7_site}{value}}"
      }
    ],
    "condition_type": "AND",
    "next": "check whether site list is empty",
    "else_eval": "${XC:COPY:{L:site_id}:{L:a_site{{id}}}"
  }
  ],
  "parse": "XMLA",
  "operation": "POST",
  "name": "send SiteConfigRequest",
  "body_list": [
    "<?xml version="1.0" encoding="UTF-8"?>",
    "<SiteConfigRequest session-id="${S::SESSID}" site-id="${L:A:site_id}"/>
  ]
  }
}


```json
{
    "op": "!=",
    "right": "${P:A:PARSE[[name]]}",
    "left": "SiteConfigResponse"
},
{
    "op": "!=",
    "right": "1",
    "left": "${P:A:PARSE[[success]]}"  
}
],
"condition_type": "OR",
"else_eval": "${XC:COPY:{L:Site}:{P:PARSE{SiteConfigResponse}}}",
"error": true
},
{
    "operation": "CONDITION",
    "name": "check operation type again",
    "condition": {
        "statements": [
            {
                "op": "==",
                "right": "${E:A:operation_type}",
                "left": "INSERT"
            }
        ],
        "condition_type": "AND",
        "eval": "${XC:COPY:{L:network}:{E:values{network}}}${XC:NETWORKTORANGE:{L:network}:{L:range}}",
        "next": "insert network"
    }
}
},
{
    "operation": "CONDITION",
    "name": "remove ip",
    "condition": {
        "statements": [
            {
                "op": "==",
                "right": "${E:A:event_type}",
                "left": "FIXED_ADDRESS_IPV4"
            }
        ],
        "condition_type": "AND",
        "eval": "${XC:COPY:{L:network}:{E:values{network}}}" + ${XC:NETWORKTORANGE:{L:network}:{L:range}}
    }
}
```

Copyright ©2019, Infoblox, Inc. All right reserved.
"condition_type": "AND",
"eval": "${XC:COPY:{L:ip}:{E:values{ipv4addr}}}${XC:REMOVEIP:{L:ip}:{L:Site{Hosts}}}",
"else_eval": "${XC:COPY:{L:ip}:{E:values{ipv6addr}}}${XC:REMOVEIP:{L:ip}:{L:Site{Hosts}}}"
},
{
  "operation": "CONDITION",
  "name": "jump to send",
  "condition": {
  "statements": [
    {
      "op": "==",
      "right": "",
      "left": ""
    }
  ],
  "condition_type": "AND",
  "next": "send SiteSaveRequest"
  }
},
{
  "operation": "VARIABLEOP",
  "name": "insert network",
  "variable_ops": [
    {
      "operation": "PUSH",
      "type": "COMPOSITE",
      "source": "L:range",
      "destination": "L:Site{Site}{Hosts}"
    }
  ]
},
{
  "parse": "XMLA",
  "operation": "POST",
  "name": "send SiteSaveRequest",
  "body_list": [
    "<?xml version="1.0" encoding="UTF-8"?>",
    "<SiteSaveRequest session-id="${S::SESSID}" />
  ]
}
"operation": "CONDITION",
"name": "send SiteSaveRequest (error check)",
"condition": {
"statements": [
{
"op": "!=",
"right": "${P:A:PARSE[[name]]}"",
"left": "SiteSaveResponse"
},
{
"op": "!=",
"right": "1",
"left": "${P:A:PARSE{{{success}}}}""
}
],
"condition_type": "OR",
"error": true
}
],
"operation": "CONDITION",
"name": "check operation type once more",
"condition": {
"statements": [
{
"op": "!=",
"right": "${E:A:operation_type}"",
"left": "INSERT"
}
],
"condition_type": "AND",
"stop": true
}
],
"operation": "PUT",
"name": "add an attribute with WAPI",
"transport":{"path": "${E:A:values{_ref}}"},
"wapi": "v2.6",
"body": "{"extattrs+": {{r7_added": {"value": "Added to the Rapid7 ${UT:A:TIME}"}}}"
Action Template: Check Operation Type

{
    "name": "check operation type",
    "operation": "CONDITION",
    "condition": {
        "statements": [
            {
                "op": "!=",
                "right": "${E:A:operation_type}",
                "left": "INSERT"
            },
            {
                "op": "!=",
                "right": "${E:A:operation_type}",
                "left": "DELETE"
            }
        ],
        "condition_type": "AND",
        "stop": true
    }
}

Note: The "check operation type" step checks the operation type. If it is neither INSERT nor DELETE, the template execution stops.

Action Template: Get the List of Sites

{
    "name": "send SiteListingRequest",
    "operation": "POST",
    "body_list": [
        "<?xml version="1.0" encoding="UTF-8"?>",
        "<SiteListingRequest session-id="${S::SESSID}" />
    ],
    "parse": "XMLA"
}

{
    "operation": "CONDITION",
    "name": "send SiteListingRequest (error check)",
    "condition": {

"statements": [{
  "op": "!=",
  "right": "${P:A:PARSE[[name]]}",
  "left": "SiteListingResponse"
},
  {  
    "op": "!=",
    "right": "1",
    "left": "${P:A:PARSE[[success]]}"  
  }  
},
"condition_type": "OR",
"error": true,
"else_eval": "${XC:COPY:{L:site_list}:{P:PARSE}"
}
}

Note: The "send SiteListingRequest" and "send SiteListingRequest (error check)
steps request the list of sites on a Rapid7 server. If the response is successful, it copies the list to the L:site_list variable.

Action Template: Locate the Site ID by Name

{  
"operation": "CONDITION",
  "name": "check whether site list is empty",
  "condition": {  
"statements": [{  
"op": "==",
  "right": "${L:L:site_list}",
  "left": "0"
}],  
"condition_type": "AND",
"stop": true
  }
},

{  
"operation": "VARIABLEOP",
  "name": "get the next site",
  "variable_ops": [{  
"operation": "POP",
  "type": "COMPOSITE",
}  
}  
}
"destination": "L:a_site",
"source": "L:site_list"
}
,
{
  "operation": "CONDITION",
  "name": "check site name",
  "condition": {
    "statements": [
      {  
        "op": ">!=",
        "right": "${L:A:a_site{{name}}}",
        "left": "${E:A:values{extattrs}{r7_site}{value}}"
      }
    ],
    "condition_type": "AND",
    "next": "check whether site list is empty",
    "else_eval": "${XC:COPY:{L:site_id}:{L:a_site{{id}}}}"
  }
}
}

NOTES:
- The "check whether site list is empty", "get the next site", and "check site name" steps form a loop for finding the site with specific name in the list of sites.
- The "check whether site list is empty" step checks to see if the list is empty. If it is empty, the site with the specific name is not found and the execution of the template stops.
- In the "get the next site" step, one element is copied to the L:a_site variable.
- In the "check site name" step, the "name" attribute of a site ("${L:A:a_site{{name}}}") is compared to the value of the "r7_site" extensible attribute of the fixed address in ("${E:A:values{extattrs}{r7_site}{value}}"). If they are the same, the site ID is stored to the L:site_id variable ("${XC:COPY:{L:site_id}:{L:a_site{{id}}}}"). If they are not the same, the execution is continued by the "check whether site list is empty" step.

Action Template: Get Site Configuration
{
  "parse": "XMLA",
  "operation": "POST",
  "name": "send SiteConfigRequest",
  "body_list": [
    "<xml version=\"1.0\" encoding=\"UTF-8\"?>",
    "<SiteConfigRequest session-id="${S::SESSID}" site-id="${L:A:site_id}"/>
  ]
},
{
  "operation": "CONDITION",
  "name": "send SiteConfigRequest (error check)",
  "condition": {
    "statements": [
      
    }
}

Copyright ©2019, Infoblox, Inc. All right reserved.
once site-id is known, steps "send SiteConfigRequest" and "send SiteConfigRequest (error check)" request and store the site configuration.

Action Template: Distinguish Between INSERT and DELETE

The "check operation type again" step determines the operation type. If the operation is "INSERT", the network of the inserted fixed address is copied to the L:network variable ${XC:COPY:{L:network}:{E:values{network}}} and transformed to a Rapid7 range to the L:range variable ${XC:NETWORKTORANGE:{L:network}:{L:range}}. After the range is stored, the template execution jumps to the "insert network" step.
Action Template: Delete an IP Address

```json
{
    "operation": "CONDITION",
    "name": "remove ip",
    "condition": {
        "statements": [{
            "op": "==",
            "right": "${E:A:event_type}",
            "left": "\$ FIXED_ADDRESS_IPV4"
        }],
        "condition_type": "AND",
        "eval": "${XC:COPY:{L:ip}:{E:values{ipv4addr}}}${XC:REMOVEIP:{L:ip}:{L:Site{Hosts}}}",
        "else_eval": "${XC:COPY:{L:ip}:{E:values{ipv6addr}}}${XC:REMOVEIP:{L:ip}:{L:Site{Hosts}}}
    }
}
```

**NOTES:**

- If the operation is not "INSERT" (i.e. "DELETE"), the "remove ip" step is executed. The step determines the type of fixed address. The corresponding address \[ {E:values{ipv4addr}} \] or \[ {E:values{ipv6addr}} \] is copied to the \$ip variable, and then the \$ip address is removed from the list of hosts in the site \( ${XC:REMOVEIP:{L:ip}:{L:Site{Hosts}}} \).
- The step "jump to send" skips the "inserting" step and jumps directly to the "send SiteSaveRequest" step.

Action Template: Add an IP Range

```json
{
    "operation": "VARIABLEOP",
    "name": "insert network",
    "variable_ops": [
```
"operation": "PUSH",
"type": "COMPOSITE",
"source": "L:range",
"destination": "L:Site{Site}{Hosts}"
]
}
}

The step "insert network" pushes the L:range to the list of site’s "Hosts".

Action Template: Saving New Configuration

{
  "parse": "XMLA",
  "operation": "POST",
  "name": "send SiteSaveRequest",
  "body_list": [
    "<?xml version="1.0" encoding="UTF-8"?>",
    "<SiteSaveRequest session-id="${S::SESSID}"",
    "${L:x:Site}",
    "</SiteSaveRequest>"
  ],
}

{
  "operation": "CONDITION",
  "name": "send SiteSaveRequest (error check)",
  "condition": {
    "statements": [
      {
        "op": "!=",
        "right": "${P:A:PARSE[[name]]}",
        "left": "SiteSaveResponse"
      },
      {
        "op": "!=",
        "right": "1",
        "left": "${P:A:PARSE{{success}}}"
      }
    ],
    "condition_type": "OR",
    "error": true
  }
}

Note: The "send SiteSaveRequest" and "send SiteSaveRequest (error check)" steps save new site configuration to the Rapid7 server.
Action Template: Add Extensible Attributes Using WAPI

```
{
    "operation": "CONDITION",
    "name": "check operation type once more",
    "condition": {
        "statements": [
            {
                "op": "!=",
                "right": "${E:A:operation_type}",
                "left": "INSERT"
            }
        ],
        "condition_type": "AND",
        "stop": true
    }
},
{
    "operation": "PUT",
    "name": "add an attribute with WAPI",
    "transport": {
        "path": "${E:A:values{_ref}}",
        "wapi": "v2.6",
        "body": "{"extattrs+": {"r7_added": {"value": \"Added to the Rapid7 ${UT:A:TIME}\"}}}"
    }
}
```

**NOTES:**
- The "check operation type once more" step determines the operation type. If the operation is not "INSERT" (i.e. "DELETE"), the template execution stops.
- For the "INSERT" operation, the last step "add an attribute with WAPI" is executed. This step adds an extensible attribute "r7_addded" to the fixed address through RESTful API. The value of the attribute has the current timestamp ($UT:A:TIME$).

Action Template: Add a Host Record

The following sample template, if assigned to a DHCP network notification rule, will insert a host record for any added network that matches the rule, with a hostname and domain name set by extensible attributes in the network. Detailed explanations about this sample are included in **Action Template with Comments: Add a Host Record**.

```
{
    "version": "1.0",
    "name": "Insert host record",
    "comment": "Will automatically insert a host record for new network insertions, assumes the network has a 'Zone' extensible attribute, optionally a 'Hostname' extensible attribute as well",
    "type": "REST_EVENT",
    "event_type": [
        "NETWORK_IPV4"
    ],
    "action_type": "Insert a host record",
    "vendor_identifier": "WAPI 2.3",
}
"transport": { "content_type": "application/json", }, "steps": [ { "name": "stop if it is not a network insert", "operation": "CONDITION", "condition": { "condition_type": "AND", "statements": [ { "left": "${E:A:operation_type}", "op": "!=", "right": "INSERT" } ], "stop": true } }, }, { "name": "stop if we don't have the zone EA set, else save it", "operation": "CONDITION", "condition": { "condition_type": "AND", "statements": [ { "left": "${E:A:values{extattrs}{Zone}{value}}", "op": "==", "right": "" } ], "stop": true, "else_eval": "${XC:COPY:{L:ZONE}:{E:values{extattrs}{Zone}{value}}}" } }, }, { "name": "get the hostname or use a default value", "operation": "CONDITION", "condition": {
"condition_type": "AND",
"statements": [
{
    "left": "${E:A:values{extattrs}{Hostname}{value}}",
    "op": "!=",
    "right": ""
},
"eval": "$\{XC:COPY:{L:HOSTNAME}:{E:values{extattrs}{Hostname}{value}}\}$",
"else_eval": "$\{XC:ASSIGN:{L:HOSTNAME}:{S:defaulthostname}\}$"
},
{
    "name": "insert the host record with the next available IP",
    "operation": "POST",
    "transport": {
        "path": "record:host"
    },
    "body_list": [
        "\{"
        "name": "$\{L:A:HOSTNAME}.\{L:A:ZONE\}\}" ,
        "\"ipv4addrs\": ["func:nextavailableip:${E:A:values{network}}"]",
        "\"comment\": "Inserted via outbound"
    ]
}
]
}

Action Template with Comments: Add a Host Record

The comments (labeled as Note:) embedded in the sample template explain the operation for each section of the template. Note that the execution of this sample template will cause a single POST request to be sent with the following body for an insertion of a 10.0.0.0/24 network with the Zone extensible attribute set to test.com and the Hostname extensible attribute set to name:

```
{"name": "name.test.com","ipv4addrs": ["func:nextavailableip:10.0.0.0/24"],"comment": "Inserted via a template"}
```

**Note:** The preamble of the template specifies the version, version, name and other relevant fields.
network has a 'Zone' extensible attribute, optionally a 'Hostname' extensible attribute as well,
"type": "REST_EVENT",

**Note:** The `event_type` field specifies that this template is used for IPv4 network events only.

"event_type": [
    "NETWORK_IPV4"
],

**Note:** The `action_type` and `vendor_identifier` fields describe the template type and the vendor type.

"action_type": "Insert a host record",
"vendor_identifier": "WAPI 2.3",

**Note:** The following specifies that the template is going to send JSON to the server.

"transport": {
    "content_type": "application/json",
},

**Note:** The following are steps that will be executed sequentially.

"steps": [

**Note:** The first step will stop the execution, without an error, if the network event received is not an insertion – it could be a modify, for example.

    {
        "name": "stop if it is not a network insert",
        "operation": "CONDITION",
        "condition": {

**Note:** You can only one statement: either AND or OR would work.

            "condition_type": "AND",
            "statements": [

**Note:** The match is to check if `operation_type` in the event is different from INSERT. It is a good practice to put the event variable on the left side so if it is not present in the event, the template would not fail.

                {
                    "left": "\${E:A:operation_type}",
                    "op": "!=",
                    "right": "INSERT"
                }
            ],

**Note:** The directive that stops the execution if the condition matches.

            "stop": true
        }
    },
}
Note: The second step will stop the execution if the inserted network does not have the Zone extensible attribute configured. If it has the extensible attribute, it will be put in a temporary local variable for easier access later on.

```json
{
    "name": "stop if we don't have the zone EA set, else save it",
    "operation": "CONDITION",
    "condition": {
        "condition_type": "AND",
        "statements": [
            {
                "left": "${E:A:values{extattrs}{Zone}{value}}",
                "op": "==",
                "right": ""
            }
        ],
        "stop": true,
        "else_eval": "${XC:COPY:{L:ZONE}:{E:values{extattrs}{Zone}{value}}}"
    }
}
```

Note: Similar to the previous section, we have only one statement, so either AND or OR would work. The condition ensures that the Zone extensible attribute is set to a value.

```json

```

Note: As previously mentioned, non-existent variable access in the left side of a condition will not cause an error, but instead return an empty value.

```json
"left": "${E:A:values{extattrs}{Zone}{value}}",
"op": "==",
"right": ""
```

Note: If the extensible attribute is empty or nonexistent, the operation should stop here.

```json
"stop": true,
```

Note: Otherwise, it will copy the zone value to the local ZONE variable.

```json
"else_eval": "${XC:COPY:{L:ZONE}:{E:values{extattrs}{Zone}{value}}}"
```

Note: This step is similar to the zone step above. However, if the host name is not set, it will put a default host name in a local variable to provide the default.

```json
{
    "name": "get the hostname or use a default value",
    "operation": "CONDITION",
    "condition": {
        "condition_type": "AND",
        "statements": [
            {
                "left": "${E:A:values{extattrs}{Hostname}{value}}",
                "op": "!=",
                "right": ""
            }
        ],
        "stop": true,
        "else_eval": "${XC:COPY:{L:ZONE}:{E:values{extattrs}{Zone}{value}}}"
    }
}
```

```json
```

Note: This step is similar to the zone step above. However, if the host name is not set, it will put a default host name in a local variable to provide the default.
"eval": "$\{XC:COPY:{L:HOSTNAME}:{E:values{extattrs}{Hostname}{value}}\}$",

Note: Otherwise, the following is executed if the extensible attribute is empty or not present, by assigning the **defaulthostname** string instead.

"else_eval": "$\{XC:ASSIGN:{L:HOSTNAME}:{S:defaulthostname}\}$"

Note: This step will finally contact the endpoint and in this case insert the host.

```
{
    "name": "insert the host record with the next available IP",
}
```

Note: This defines the HTTP operation to use.

"operation": "POST",

Note: The endpoint is configured starting with **https://master_ip/**. The endpoint template overrides the path with **/wapi/v2.3/** so by default all template requests would go to **https://master_ip/wapi/v2.3/**. In this step, we want to insert a host, so **record:host** is appended to the URI above (no override is set here) to arrive to the valid RESTful URI **https://master_ip/wapi/v2.3/record:host**.

```
"transport": {
    "path": "record:host"
},
```

Note: This is the text that will be sent to the server in the POST’s BODY.

```
"body_list": [
    "\n"name\": \"${L:A:HOSTNAME}.${L:A:ZONE}\",",
    "ipv4addrs": ["func:nextavailableip:${E:A:values{network}}"]],",
```

Note: This option signifies that the RESTful API will use the next available IP in the network as the address for this host.

```
"comment": "Inserted via outbound",
"\n"\n"
```

Note: This chapter provides information about the Infoblox Threat Insight (also referred to as Threat Analytics in Grid Manager), which protects mission-critical DNS infrastructure from data exfiltration through DNS tunneling.
This chapter includes the following sections:

- About Data Exfiltration
- About Infoblox Threat Insight
- About Infoblox Threat Insight
- Guidelines for Using Infoblox Threat Insight
- Supported Appliances for Infoblox Threat Insight
- Configuring Infoblox Threat Insight
- Starting and Stopping the Threat Analytics Service
- Viewing the Analytics Whitelist
- Adding Custom Whitelisted Domains
- Configuring a Local RPZ as the Mitigation Blacklist Feed
- Enabling Threat Insight for the Cloud Client
- Viewing Blacklisted Domains
- Moving Blacklisted Domains to the Whitelist
- Monitoring DNS Tunneling Activities

About Data Exfiltration

The DNS protocol is increasingly used as a pathway for data exfiltration through DNS tunneling attacks. DNS tunneling involves tunneling another protocol through port 53 — often not inspected by firewalls (even the next-generation firewalls) — by malware-infected devices or malicious insiders. There are a number of tools available for tunneling over DNS for a common motivation of bypassing captive portals for paid Wi-Fi access. A free tunneling application released under the ISC license for forwarding IPv4 traffic through DNS servers is one example of the software used in this kind of attack.

As illustrated in Figure 43.1, sensitive information such as credit card numbers and company financial can be stolen either by establishing a DNS tunnel from within the network or by encrypting and embedding chunks of that data in DNS queries. Data is decrypted at the other end and put back together so valuable information can be stolen and misused by malicious attackers.

Figure 43.1 Data Exfiltration

You can use the following features to specifically target DNS tunneling traffic and minimize the risk of DNS data exfiltration:

- Anti-DNS tunneling threat protection rules: These rules detect signature-based payload encoding techniques, such as Base32, Base64 and suspicious label lengths, commonly used by tunneling products such as OzymanDNS, Iodine, DNS2TCP, and SplitBrain. For more information about the threat protection rules, refer to the Threat Protection Rules document available on the Infoblox Support site.
- Infoblox Threat Insight: Infoblox employs streaming analytics to study DNS statistics and create algorithms to identify DNS tunneling traffic. To further defend your system against DNS data exfiltration, Infoblox Threat Insight detects and mitigates DNS tunneling traffic by analyzing DNS queries and responses. Infoblox Threat Insight constantly evaluates incoming DNS traffic and
Following are some guidelines to take into consideration when using Infoblox Threat Insight:

- To start the threat analytics service, you must have at least one RPZ license installed in your Grid (it can be installed on any Grid member) and the Threat Analytics license installed on the Grid member on which you want to start the threat analytics service. To download updates for threat analytics module and whitelist sets, you must have at least one Threat Analytics license installed in the Grid.

- Infoblox recommends that you run the threat analytics service for a limited time to monitor and preview what has been detected before actually blocking blacklisted domains. You can carefully review the list of detected domains and decide which domains you want to continue blocking and which domains you want to add to the analytics whitelist. You should review the blacklisted domains on a regular basis to ensure they are still relevant and the list is not growing due to new threats or changing network environments.

About Infoblox Threat Insight

To mitigate DNS data exfiltration, Infoblox Threat Insight (also referred to as Threat Analytics in the Infoblox GUI or Grid Manager) employs analytics algorithms to detect DNS tunneling traffic by analyzing incoming DNS queries and responses. These algorithms are developed through an extensive study and analysis of sample DNS statistics within which DNS tunneling data is identified by algorithms that cannot be detected by normal rules and signatures. For more information about these analytics, see About Data Exfiltration.

Infoblox Threat Insight identifies data exfiltration tunnels that bypass typical firewall systems. Some popular tunneling tools are OyzmanDNS, SplitBrain, Iodine, DNS2TCP, TCP-Over-DNS, and others. This type of DNS threats are identified as having high activities by using the TXT records in DNS queries. Infoblox Threat Insight also identifies tunnels that are used for C&C. These threats typically do not exhibit high activities or payloads. In general, NXDOMAIN responses fall into this category of threats.

You must have at least one RPZ license installed in your Grid (it can be installed on any Grid member) and the Threat Analytics license installed on the Grid member on which you want to start the threat analytics service. To download updates for threat analytics module and whitelist sets, you must have at least one Threat Analytics license installed in the Grid. When you enable the threat analytics service, NIOS starts analyzing incoming DNS data and applying these algorithms to detect security threats that have the same or similar behavior as the known data. Once security threats are detected, NIOS blacklists the domains and transfers them to the designated mitigation RPZ (Response Policy Zone), and traffic from the offending domains is blocked and no DNS lookups are allowed for these domains from NIOS members on which RPZ are assigned to them. The appliance also sends an SNMP trap each time it detects a new blacklisted domain.

Infoblox Threat Insight also includes a whitelist that contains trusted domains on which NIOS allows DNS traffic. These are known good domains that carry legitimate DNS tunneling traffic such as Avast, Sophos, McAfee, Boingo, Barracuda, and others. The whitelist is extensible so new whitelisted domains can be added and rolled out accordingly.

You can also add custom whitelisted domains or move blacklisted domains to the whitelist. For more information about how to configure Infoblox Threat Insight, see Configuring Infoblox Threat Insight. Before you utilize Infoblox Threat Insight, there are a few guidelines you might need to consider. For more information, see Guidelines for Using Infoblox Threat Insight.

Infoblox Threat Insight came installed with a module set and a whitelist set. To receive subsequent module set and whitelist set updates, you can configure the appliance to automatically download and apply the updates for you, or you can manually upload the updates when the appliance displays a banner message notifying about available updates. For information about how to configure the update policy, see Defining the Threat Analytics Update Policy.

Licensing Requirements and Admin Permissions

You must obtain and install valid licenses on your appliance before using Infoblox Threat Insight. Contact your Infoblox representative to obtain these licenses. For more information, see Managing Licenses.

Infoblox Threat Insight

To start the threat analytics service, you must have at least one RPZ license installed in your Grid (it can be installed on any Grid member) and the Threat Analytics license installed on the Grid member on which you want to start the threat analytics service. To download updates for threat analytics module and whitelist sets, you must have at least one Threat Analytics license installed in the Grid.

Note that running the threat analytics service might affect your system performance if the appliance has a small capacity and is taking on heavy traffic. Evaluate your Grid and Grid members to ensure that you select an appliance that is appropriate for running the threat analytics service. For supported appliances, see Supported Appliances for Infoblox Threat Insight.

Admin Permissions

Superusers can configure all threat protection and analytics related tasks. You can assign Security Permissions to specific admin groups and roles so these users can configure security related tasks. You can also add a global permission for managing Grid security properties or add an object permission for managing member security properties.

To manage the analytics related tasks, you must assign appropriate read-only or read/write Analytics Permissions to the specified admin groups and roles. You can also add the Global Analytics Permission as a global permission or add Member Analytics Permission to specific Grid members as an object permission.

For more information about how to assign admin permissions, see Managing Permissions.
To configure Infoblox Threat Insight, complete the following:

1. Obtain and install valid RPZ and Threat Analytics licenses on the appliance that is used to support analytics. For more information about licenses, see About Infoblox Threat Insight. Note that you must have the threat analytics service running on the member serving recursive DNS queries or have recursive DNS queries forwarded to another DNS server. To generate reports that contain statistics about DNS tunneling, you must also configure a reporting appliance in the Grid.

2. Create and add a new RPZ and use it as the designated mitigation blacklist feed so the appliance can transfer all blacklisted domains to this feed. For more information, see Configuring a Local RPZ as the Mitigation Blacklist Feed. Ensure that you configure an appropriate policy for this RPZ. To monitor the threat analytics service before actually blocking domains, set Policy Override to Log Only (Disabled) . When you are ready to block offending domains, set Policy Override to None (Given).

3. Configure admin permissions so admin users can manage the threat analytics service and analytics related tasks. For information about how to configure admin permission, see Managing Permissions.

4. Start the threat analytics service on the appliance that has the Threat Analytics license installed, as described in Starting and Stopping the Threat Analytics Service.

Note: The analytics functionality only works on recursive servers and forwarding servers that use BIND as the DNS resolver; it does not function on authoritative servers or servers that use Unbound as the DNS resolver.

After you set up Infoblox Threat Insight to mitigate DNS data exfiltration, you can do the following to manage it:

- View supported whitelisted domains for analytics, as described in Viewing the Analytics Whitelist. Note that these domains are specific to analytics only. They are not used in the anti-DNS tunneling threat protection rules.
- Manually add a custom domain to the analytics whitelist, as described in Adding Custom Whitelisted Domains.

Supported Appliances for Infoblox Threat Insight

Due to memory and capacity required to perform analytics, ensure that you install the Threat Analytics and RPZ licenses, and enable the threat analytics service on an appliance that has a big enough capacity. Following are the supported Infoblox appliance models on which you can run the threat analytics service:

- PT-1405, PT-2200, PT-2205, and PT-4000.
- IB-4010, IB-4030 and IB-4030-10GE.
- TE-1415, TE-1425, TE-2210, TE-2215, TE-2220, and TE-2225.
- TE-V1415, TE-V1425, TE-V2210, TE-V2215, TE-V2220, TE-V2225, TE-V4010 and TE-V4015.

Note: Using unsupported appliance models for Infoblox Threat Insight might cause performance issues.

Copyright ©2019, Infoblox, Inc.All right reserved.
• Review the blacklisted domains and make decisions about whether to move them to the analytics whitelist so future DNS activities will not be blocked. For more information, see Viewing Blacklisted Domains.
• Move a blacklisted domain to the analytics whitelist, as described in Moving Blacklisted Domains to the Whitelist.
• Monitor DNS tunneling activities and events using pre-defined reports and the syslog, as described in Monitoring DNS Tunneling Activities.

Starting and Stopping the Threat Analytics Service

To start the threat analytics service, you must have at least one RPZ license installed in your Grid (it can be installed on any Grid member) and the Threat Analytics license installed on the Grid member on which you want to start the threat analytics service. You can also stop the service when necessary.

To start or stop the threat analytics service:

1. From the Grid tab, select the Grid Manager tab -> Services tab, click the Threat Analytics service link. Grid Manager displays only the member or members with the RPZ license installed. Select the member check box.
2. From the Toolbar, click Start to start the service or Stop to stop the service.

When you stop the threat analytics service, the appliance does not detect or protect against non-signature-based DNS tunneling. In addition, reports that you generate might not include statistics related to DNS tunneling.

Note: After you enable the threat analytics service, you must restart DNS service for the analytics to start working.

Viewing the Analytics Whitelist

The Data Management tab -> Threat Analytics tab -> Whitelist tab of Grid Manager lists the trusted domains on which NIOS allows DNS traffic by default. These are known good domains that carry legitimate DNS tunneling traffic such as Avast, Sophos, McAfee, Boingo, Barracuda, and others. They are marked as System domains, and you cannot delete them; but you can disable them so NIOS does not treat them as trusted domains. You can also add custom domains or move blacklisted domains to the analytics whitelist. For more information, see Adding Custom Whitelisted Domains and Moving Blacklisted Domains to the Whitelist.

To view a complete list of trusted domains in the analytics whitelist:

1. From the Data Management tab, select the Threat Analytics tab -> Whitelist tab.
2. The appliance displays the following for each trusted domain:
   • **Actions:** Click the Action icon (shown as a gear in each row) next to a domain and select one of the following:
     • **Disable:** Click this to disable the domain. When you disable a domain, the appliance does not treat this domain as trusted domain until you enable it.
     • **Edit:** Click this to open the Whitelist editor. For system domains, the only property you can modify is to disable or enable them. For custom domains however, you can also add information to the Comment field.
     • **Delete:** This is only applicable to custom domains. You cannot delete system domains. Select this to delete the custom domain.
   • **Domain Name:** The name of the trusted domain.
   • **Type:** Displays the domain type. This can be System or Custom. A system domain is a trusted domain that carries legitimate DNS tunneling traffic such as Avast, Sophos, McAfee, Boingo, Barracuda, and others. A custom domain is one that you have added to the whitelist or moved from the mitigation blacklist RPZ.
   • **Disabled:** Indicates whether this domain is disabled or not. The appliance does not treat disabled domains as trusted domains.
   • **Comment:** Additional information about the domain.

Note: When you upgrade to a future NIOS release or update the analytics whitelist, all changes made to the whitelist will be preserved.

You can also do the following in this panel:

• Click Go to Mitigation Response Policy Zone to access the blacklisted domains that are identified as offenders for DNS tunneling. Blacklisted domains are detected through Infoblox Threat Insight and automatically transferred to the blacklist RPZ feed. For information about these domains, see Viewing Blacklisted Domains.
• Export or import whitelisted domain names using the CSV import and export functionality.
• Navigate to the next or last page of the whitelist using the paging buttons at the bottom of the panel.
• Refresh the analytics whitelist by clicking the Refresh button.
• Use filters and the Go to function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Go to field and select the object from the possible matches.
• Select a quick filter to search for System or Custom whitelist entries, or both.
• Print the whitelist or export it in CSV format.
Adding Custom Whitelisted Domains

The analytics whitelist is populated with trusted domains that carry legitimate DNS tunneling traffic such as Avast, Sophos, McAfee, Boingo, Barracuda, and others. For more information, see Viewing the Analytics Whitelist. You can add domains that you deem trustworthy to this list. When you add a custom domain, it is marked as Custom in the whitelist.

To add a custom whitelisted domain, complete the following:

1. From the Data Management tab, select the Threat Analytics tab -> Whitelist tab, click the Add icon or click Add Custom Whitelist from the Toolbar.
2. In the Add Custom Whitelist wizard, complete the following:
   - **Domain Name**: Enter the name of the domain that you want to add to the analytics whitelist.
   - **Comment**: Enter additional information about this domain.
   - **Disable**: When you select this, the appliance does not treat this domain as a trusted domain. When you enable the domain again, it is considered as a whitelisted domain.
3. Save the configuration. You do not need to restart DNS service to update the analytics whitelist.

Configuring a Local RPZ as the Mitigation Blacklist Feed

For the threat analytics service to function properly and for NIOS to properly report detected backlisted domains, you must create and designate local RPZs as the mitigation for the Grid. You can add any Response Policy Zones to the list of RPZs from different Network and DNS Views. When a domain is detected as malicious, NIOS will update all RPZs in the list. If you assign an existing RPZ that is used for other purposes as the mitigation blacklist feed, you may experience the following:

- Existing RPZ hits are reported as hits detected by the analytics after an upgrade.
- If you manually add rules to the RPZ, all RPZ hits are reported as hits detected by the analytics, regardless of whether they match the manually created rules or are detected through the threat analytics service.

Infoblox recommends that you run the threat analytics service for a limited time to monitor and preview what has been detected before actually blocking domains. To do so, set Policy Override to Log Only (Disabled) when you create the RPZ so you can monitor blacklisted domains without actually blocking them.

**Note**: You can designate only one local RPZ as the Grid-wide mitigation blacklist feed.

To create and designate a local RPZ as the blacklist feed:

1. Create a local RPZ by completing the procedure described in Configuring Local RPZs.

   **Note**: To monitor the threat analytics service without blocking domains, set Policy Override to Log Only (Disabled). When you are ready to block blacklisted domains, set Policy Override to None (Given).

2. From the Data Management tab, select the Threat Analytics tab -> Whitelist tab, click the Grid Threat Analytics Properties from the Toolbar.
3. In the Grid Threat Analytics Properties editor, click the DNS Threat Analytics tab, and complete the following:
   - Click the Add icon to open the Zone Selector dialog box and select the RPZs. You must configure at least one local RPZ. To remove an RPZ, select it from the table and click Delete.
4. Save the configuration.

   **Note**: You cannot delete an RPZ that is used as the mitigation blacklist feed until you remove or clear it from the Grid Threat Analytics Properties editor.

Enabling Client for Threat Insight in the Cloud

If your network configuration includes ActiveTrust Plus or ActiveTrust Advanced Cloud, you can configure a cloud integration client to collect malicious domains detected by the Threat Insight in the cloud. NIOS then applies the detected domains to RPZs that were configured for the on-premises Grid. This feature ensures that all malicious domains detected in the cloud are also captured for on-premises members.

You can use this feature when you have ActiveTrust Plus or ActiveTrust Advanced license. Note that you can configure only one cloud client per on-premises Grid and you must first request an API key through the Cloud Services Portal, so that the cloud client is authorized to retrieve data from Threat Insight in the Cloud.

To configure Threat Insight for the cloud client:

1. From the DataManagement tab, select the DNS tab -> Response Policy Zones tab. Expand the Toolbar and click Threat insight in the Cloud Client.
2. In the Threat insight in the Cloud Client editor, complete the following:
   - **Enable Cloud Client**: Select this check box to enable Threat Insight results in the cloud client.
The Appliance Key: You must request an API key to establish an authorized connection with the cloud client. Click **Request API Key** to request an API key. Do the following in the Request API Key from the **Cloud Services Portal** dialog box:

- **Email:** Enter the email address that is registered in the Infoblox Cloud Services Portal.
- **Password:** Enter the password that is registered in the Infoblox Cloud Services Portal.

An API key is generated in the **API Key** text box only when you enter the correct email address and password. An error message is displayed for an invalid email address and password.

- **Interval:** You can specify how often to request Threat Insight results detected in the cloud client in seconds or minutes. The default is 10 minutes.

- **The list of Response Policy Zones to use for blacklisted domains:** Click the Add icon to add an RPZ to the list. Whenever there are multiple zones, Grid Manager displays the **Zone Selector** dialog box from which you can select one. You can add an RPZs from different network and DNS views. Whenever a new RPZ is added and the cloud client requests data, Grid Manager displays a Warning dialog box to confirm that you wish to request all detected domains by Threat Insight in the cloud client. Even if you have clipped **No** in the **Warning** dialog box, you can use the set cloud_services_portal_force_refresh CLI command in maintenance mode and set the flag to request all domains detected in the cloud client.

3. Click **Save & Close**.

**Viewing Blacklisted Domains**

To review the list of blacklisted domains, complete the following:

1. From the **Data Management** tab, select the **Data Management** tab -> **DNS** tab -> **Response Policy Zones** tab, click the mitigation blacklist RPZ name.
2. Grid Manager displays the following for each blacklisted domain:
   - **Name or Address:** Displays the name or IP address of the blacklisted domain.
   - **Policy:** Displays the policy used to handle the responses when NIOS detected the blacklisted domain.
   - **Data:** Displays the target data about this domain.
   - **Comment:** Displays additional information about this domain.
   - **Site:** This is a pre-defined extensible attributes (if configured) that is used to indicate the location of the domain.
   - **Disable:** Indicates whether this domain is disabled or not. When the domain is disabled, the appliance does not block activities on this domain, and configuration for this domain does not change. When the domain is enabled, it is considered as a blacklisted domain and all DNS activities are blocked.

You can also do the following in the blacklisted domain panel:

- Click **Go to Analytics Whitelist View** to view the analytics whitelist. In the Whitelist panel, you can see all the trusted domains for Infoblox Threat Insight, and DNS activities are allowed on these domains. For more information, see Viewing the Analytics Whitelist.

- If you want to move a blacklisted domain to the analytics whitelist so it becomes a trusted domain, select the domain check box and click the Action icon

  (shown as a gear in each row) next to the domain, and then select **Move to Whitelist**.

  - Navigate to the next or last page of the whitelist using the paging buttons at the bottom of the panel.
  - Refresh the blacklist feed by clicking the Refresh button.
  - Use filters and the **Go to** function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the **Go to** field and select the object from the possible matches.
  - Select a quick filter to search for specific entries.
  - Print the blacklist or export it in CSV format.

**Moving Blacklisted Domains to the Whitelist**

When the appliance detects an offending domain for possible DNS tunneling, it responses according to the policy defined in the mitigation blacklist RPZ and adds the domain to the blacklist RPZ feed. You can view all blacklisted domains and turn those you deem trustworthy into trusted domains by moving them to the analytics whitelist. Note that once you move a blacklisted domain to the whitelist, you cannot reverse the action.

To move a blacklisted domain to the analytics whitelist:

1. From the **Data Management** tab, select the **Data Management** tab -> **DNS** tab -> **Response Policy Zones** tab.
2. Select a blacklisted domain and click the Action icon

  (shown as a gear in each row) next to a domain and select **Move to Whitelist**.

The appliance removes the selected domain from the blacklist and adds it to the analytics whitelist. You can click **Go to Analytics Whitelist View** to verify that the domain has been successfully moved.

**Updating Threat Analytics Module and Whitelist Sets**
Infoblox periodically releases threat analytics module and whitelist sets. To ensure that you can import threat analytics updates, you must have at least one Threat Analytics license installed in the Grid. The threat analytics module set consists of the analytics application .jar file, which delivers changes and updates for DNS tunneling detection; and the whitelist set consists of updated trusted domains that carry legitimate DNS tunneling traffic. You can download updates for the module set and whitelist set independently depending on how often Infoblox rolls them out. The appliance displays the version numbers of the module set and whitelist set that your Grid is currently using. To view this information before downloading updates, see Viewing Module and Whitelist Versions.

You can configure the appliance to automatically receive and apply the latest module set and/or whitelist set. When you define an automatic update policy, the appliance checks both the analytics module and whitelist files and automatically downloads the files that have changed. You can also configure a manual update policy in which the appliance notifies you through the message banner when there are updates available. You can then decide whether you want to apply the updates to your Grid or not. For information about how to define the update policy, see Manually Uploading Threat Analytics Updates.

Note: Note that only the Grid Master receives module set and whitelist set updates. Grid member receives these updates through standard Grid replication from the Grid Master. Module and whitelist data is only replicated to Grid members that have the threat analytics service enabled (an RPZ license is required to start this service on the members). The appliance uses the port 443 (HTTPS) for downloading the module set and whitelist data updates.

Infoblox recommends that you configure the appliance to automatically receive module and whitelist updates so your appliance receives the latest information periodically. If you prefer to manually upload updates to your Grid, ensure that you apply them frequently to receive the most updated information.

Viewing Module and Whitelist Versions

1. From the Data Management tab, select the Threat Analytics tab -> Whitelist tab, click the Grid Threat Analytics Properties from the Toolbar.
2. In the Grid Threat Analytics Properties editor, click the Updates tab. This tab displays the following information:
   - Current Whitelist Version: Displays the version number of the threat analytics whitelist set that is currently running on the Grid.
   - Active Module Set Version: Displays the version number of the threat analytics module set that is currently active on the Grid.

Defining the Threat Analytics Update Policy

To configure how you want to obtain the latest threat analytics updates, complete the following:

1. From the Data Management tab, select the Threat Analytics tab -> Whitelist tab, click the Grid Threat Analytics Properties from the Toolbar.
2. In the Grid Threat Analytics Properties editor, click the Updates tab,
3. In the Module Set Updates section, complete the following:
   - Latest Available Module Set: Displays the latest module set that is available for download.
   - Last Checked For Updates: Displays the timestamp when the Grid last checked for updates.
   - Module Set Update Policy: When you select Automatic, the appliance automatically downloads the latest module set and/or whitelist set based on the default or custom schedule. The appliance checks both the module and whitelist files and automatically downloads only the files that have changed. When you select an automatic policy, the threat analytics service on the Grid members is restarted automatically to activate the latest updates. If you select Manual as the update policy, the appliance displays a banner message in Grid Manager to notify you when a new update is available. You must then decide whether to apply the updates to the Grid or not. For information about how to manually apply the updates, see Manually Uploading Threat Analytics Updates.
   - Enable Automatic Module Set Updates: Select this check box to enable the automatic upload feature. When necessary, you can click Download Module Set Now to override the automatic update policy.

In the Schedule section, select one of the following to set up a recurring schedule for automatic downloads:

- **Default**: When you select this, the appliance downloads the updates between 12:00 a.m. and 6:00 a.m. local time based on the time zone configured on your appliance. The appliance automatically selects a time between this time window the first time it performs an automatic update. All subsequent updates then follow the same schedule based on the selected time.
- **Custom**: Select this and click the calendar icon to configure a custom schedule. In the Automatic Module Set Updates Scheduler, you can select Hourly, Daily, Weekly, or Monthly based on how often you want to update the module set and whitelist set.

Note: The scheduled time does not indicate the exact time for the download. Downloads occur during the mid-point during of a 30-minute time frame. Therefore, the actual download can happen 15 minutes before or after the scheduled time.

When you select **Hourly**, complete the following:

- **Schedule every hour(s) at**: Enter the number of hours between each update instance. You can enter a value from 1 to 24.
- **Minutes past the hour**: Enter the number of minutes past the hour. For example, enter 5 if you want to schedule the rule update five minutes after the hour.
- **Time Zone**: Select the time zone for the scheduled time from the drop-down list.

When you select **Daily**, you can select either **Every day** or **Every Weekend** and then complete the following:
1. Time: Enter a time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.

2. Time Zone: Select the time zone for the scheduled time from the drop-down list. When you select Weekly, complete the following:

   - Schedule every week on: Select any day of the week.
   - Time: Enter a time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.

3. Time Zone: Select the time zone for the scheduled time from the drop-down list. When you select Monthly, complete the following:

   - Schedule the day of the month: Enter the day of the month and the monthly interval. For example, to schedule the rule update on the first day after every 2 months, you can enter Day 1 every 2 month(s).
   - Time: Enter a time in hh:mm:ss AM/PM (hours:minutes:seconds AM or PM) format. You can also select a time from the drop-down list by clicking the time icon.

4. Time Zone: Select the time zone for the scheduled time from the drop-down list.

4. Save the configuration.

Manually Uploading Threat Analytics Updates

When you configure a manual update policy, the appliance notifies you about newly available module set and/or whitelist set updates. You can manually upload the updated files and apply them to the Grid.

To manually upload threat analytics updates:

1. From the Data Management tab, select the Threat Analytics tab -> Whitelist tab, click Updates -> Manual Update from the Toolbar.

2. The Threat Analytics Upload dialog displays the following:

   - Current Whitelist Version: Displays the version of the whitelist set that is currently running on the Grid.
   - Last Applied On: Displays the timestamp and time zone when the last whitelist set was applied to the Grid. This field changes each time when a whitelist set is applied.
   - Latest Available Module Set: Displays the version string of the latest available module set. This field changes each time when the module set is updated.
   - Last Applied On: Displays the timestamp and time zone when the last module set was applied to the Grid. This field changes each time when a module is applied.

To upload the module set or whitelist set:

- File: Click Select to navigate to the file location, and then upload the file. The appliance displays the file name in this field. You can upload either a module set or a whitelist set. Check the current version numbers of the whitelist and module sets to verify if they have changed before uploading new files.

Note: You can only update to a newer whitelist set even though you can switch back to an older version of module set, if any. However, if you have configured an Automatic update policy, the appliance overwrites the older file version with the new one. To avoid this, you can change the update policy to Manual or disable automatic downloads.

Click Test to check the changes that will occur during the update, without actually applying the update. You can view update details in the Syslog Viewer. The appliance preserves the uploaded file if you do not click Update to update the module set or whitelist set. When you manually upload next time, this file name is displayed in the dialog. You can then choose to apply the update from this file or upload a new file before performing the update. Uploading a new file will remove the file that has not been applied.

3. Click Update to update the module set or whitelist set. You can also click View Update Results to view the update results.

Monitoring DNS Tunneling Activities

You can monitor DNS tunneling activities through the following:

- Pre-defined Reports: If you have a reporting appliance configured in the Grid, you can generate the following reports that include DNS tunneling data:
  - DNS Top Tunneling Activity
  - DNS Tunneling Traffic by Category
  - Top Malware and DNS Tunneling Events by Client

- Syslog: All DNS tunneling activities are logged to the syslog. You can view this log to identify specific activities related to DNS tunneling. For more information, see Using a Syslog Server.

Part 9 Reference

This section provides reference information in the following appendices:
The following table provides descriptions of some key terminology used in the Infoblox products. Some terms, such as Grids and high availability, are used in different ways by other networking product vendors. The alphabetically arranged table can help you understand the terms and concepts as Infoblox uses them and as they are used in this guide.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Node</td>
<td>The NIOS appliance in an HA (high availability) pair that receives, processes, and responds to all service requests. When an HA failover occurs, the active node becomes the passive node in the HA pair.</td>
</tr>
<tr>
<td>API (Application Programming Interface)</td>
<td>A set of rules and specifications that software programs follow to communicate with each other. It serves as an interface between different software programs and facilitates their interaction. Infoblox provides a Perl API to help facilitate the integration of Infoblox NIOS appliances into network environments. It is an alternate method to the GUI (graphical user interface) in which you use a mouse pointer to click and select options and items to perform tasks.</td>
</tr>
<tr>
<td>Authenticated DHCP</td>
<td>The process of authenticating a network device before a DHCP server assigns a lease. On Infoblox appliances, you can divide a network into segments for unauthenticated, authenticated, and guest users. The Infoblox DHCP server assigns clients to the appropriate segment based on their MAC addresses and authentication credentials.</td>
</tr>
<tr>
<td>BIND (Berkeley Internet Name Domain)</td>
<td>The most commonly used DNS server on the Internet. It allows for a standard way of naming objects and resource records in distributed UNIX environments. It also provides operations for storing and retrieving information about these objects and records.</td>
</tr>
<tr>
<td>bloxSYNC</td>
<td>An Infoblox proprietary mechanism for secure, real-time synchronization of the database that maintains the data, system configuration, and protocol service configuration between the active and passive nodes of an HA pair. With bloxSYNC, the nodes continuously synchronize changes of their configurations and states. When a failover occurs, the passive node can quickly take over services from the active node.</td>
</tr>
<tr>
<td>bloxTools</td>
<td>An Infoblox pre-installed environment that provides tools for creating custom applications that facilitate administrative tasks for an organization.</td>
</tr>
<tr>
<td>Bucket</td>
<td>A bucket contains indexed data.</td>
</tr>
<tr>
<td>Bulk Host</td>
<td>If you need to add a large number of A and PTR records, you can have the NIOS appliance add them as a group and automatically assign host names based on a range of IP addresses and the host name format you specify. Such a group of records is called a bulk host, which the appliance manages and displays as a single bulk host record.</td>
</tr>
<tr>
<td>Captive Portal</td>
<td>An Infoblox service that you enable on Grid members to register users, guest users, or both types of users for authentication purposes on network segments that you define using the authenticated DHCP feature.</td>
</tr>
<tr>
<td><strong>CIDR (Classless Inter-Domain Routing) Notation</strong></td>
<td>A compact specification of an IPv4 or IPv6 address and its associated routing prefix. For example, the CIDR notation of 192.168.100.1/24 represents the IPv4 address of 192.168.100.1 and its routing prefix of 192.168.100.0, or its subnet mask of 255.255.255.0. The CIDR notation of 2001:DB8::/48 represents the IPv6 addresses from 2001:DB8:0:0:0:0:0:0 to 2001:DB8:0:FFFF:FFFF:FFFF:FFFF:FFFF.</td>
</tr>
<tr>
<td><strong>CLI (Command-line Interface)</strong></td>
<td>A way to interact with Infoblox products by typing text-only commands to perform specific tasks.</td>
</tr>
<tr>
<td><strong>Cluster Grouping</strong></td>
<td>Grouping reporting appliances as a disaster recovery measure.</td>
</tr>
<tr>
<td><strong>Dashboard</strong></td>
<td>Your home page on Infoblox Multi-Grid Manager, Grid Manager, and System Manager. It provides easy access to tasks and to the status of your Grids and networks. It also provides various widgets for viewing and managing data.</td>
</tr>
<tr>
<td><strong>DDNS (Dynamic DNS)</strong></td>
<td>The automatic updating of real-time DNS configuration changes and other information on a DNS server when a network device is assigned a new IP address.</td>
</tr>
<tr>
<td><strong>DHCP (Dynamic Host Configuration Protocol)</strong></td>
<td>A configuration protocol that provides address assignments to network devices within a network. It keeps track of network configuration for each network device.</td>
</tr>
<tr>
<td><strong>DHCP Failover Association</strong></td>
<td>The pairing of two DHCP servers that establish a TCP connection for their communications. The servers form a pair of DHCP failover peers and provide DHCP protocol redundancy to minimize DHCP service outages.</td>
</tr>
<tr>
<td><strong>DHCP Filter</strong></td>
<td>A set of criteria and rules used to screen requesting hosts by matching MAC addresses, relay agent identifiers, DHCP options, or RADIUS authentication results.</td>
</tr>
<tr>
<td><strong>DHCP Template</strong></td>
<td>A set of predefined properties that you use to create IPv4 and IPv6 DHCP objects, such as networks and DHCP ranges, on the Infoblox appliance.</td>
</tr>
<tr>
<td><strong>DIW (Data Import Wizard)</strong></td>
<td>An Infoblox software tool that facilitates the import of DNS, DHCP, and TFTP data from legacy servers to Infoblox NIOS appliances. DIW supports DNS data import in the following formats: BIND 9, BIND 8, BIND 4, Microsoft DNS, Lucent VitalQIP, and Nortel NetID. It supports DHCP data import in the following formats: ISC DHCP, Microsoft DHCP, Lucent VitalQIP, and Nortel NetID.</td>
</tr>
<tr>
<td><strong>DNS (Domain Name System)</strong></td>
<td>A hierarchical naming system that translates domain names of any network devices into IP addresses for the purpose of locating and addressing these devices worldwide.</td>
</tr>
<tr>
<td><strong>DNS View</strong></td>
<td>On Infoblox appliances, a DNS view provides the ability to serve one version of DNS data to one set of clients and another version to another set of clients. With DNS views, the Infoblox appliance can provide a different answer to the same DNS query, depending on the source and match destinations of the query.</td>
</tr>
<tr>
<td><strong>DNSSEC (Domain Name System Security Extensions)</strong></td>
<td>A suite of IETF (Internet Engineering Task Force) specifications for securing certain kinds of information provided by DNS for use on IP networks. It is a set of extensions to DNS, which provide DNS resolvers with the original authentication of DNS data, authenticated denial of existence, and data integrity.</td>
</tr>
<tr>
<td><strong>DNSone™</strong></td>
<td>The software package that enables Infoblox appliances to provide DNS, DHCP and TFTP services. You can add the Grid upgrade to Infoblox appliances running DNSone.</td>
</tr>
<tr>
<td><strong>Endpoint</strong></td>
<td>An IP device such as a personal computer, laptop, or mobile handheld device. This term is often used in a security context.</td>
</tr>
<tr>
<td><strong>Extensible Attribute</strong></td>
<td>Metadata you define to capture additional information about an object managed by the Infoblox NIOS appliance. You can use predefined attributes or create your own. You can also specify required attributes and restrict the values that users can enter for each attribute.</td>
</tr>
<tr>
<td>Filters</td>
<td>Criteria the Infoblox NIOS appliance uses to request specific information in the database. You can use filters to control the amount and the kind of data displayed in a panel or table in Infoblox Multi-Grid Manager, Grid Manager, and System Manager.</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FQDN (fully qualified domain name)</td>
<td>A complete domain name that specifies its exact location in the hierarchy of the DNS. It specifies all the domain levels, including the top-level domain and the root domain.</td>
</tr>
<tr>
<td>FTP (File Transfer Protocol)</td>
<td>A standard network protocol used to transfer files from one network device to another over a TCP-based network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server.</td>
</tr>
<tr>
<td>Gateway</td>
<td>The default router for the immediate network segment of an interface.</td>
</tr>
<tr>
<td>Grid™ Technology</td>
<td>Infoblox’s unique and patented high availability Grid technology ensures network reliability. The Infoblox Grid provides resilient network services, failover, recovery, and seamless maintenance for an Infoblox deployment inside a single building, across a networked campus, or between remote locations. The Infoblox Grid establishes a distributed relationship between individual or paired appliances to remove single points of failure and other operational risks inherent in legacy DNS, DHCP, and IP address management infrastructure.</td>
</tr>
<tr>
<td>Grid Manager</td>
<td>The NIOS web interface that provides access to your Grid for performing IPAM, DNS, and DHCP management and other administration tasks.</td>
</tr>
<tr>
<td>Grid Master</td>
<td>The Grid member in an Infoblox Grid that maintains the NIOS database that is distributed among all members of the Grid. You connect to the Grid Master to configure and monitor the entire Grid.</td>
</tr>
<tr>
<td>Grid Member</td>
<td>Any single Infoblox NIOS appliance or HA pair that belongs to a Grid. Each member can use the data and services of the Grid. You can also modify settings so that a Grid member can use unique data and member-specific services.</td>
</tr>
<tr>
<td>HA Pair</td>
<td>Two physical Infoblox NIOS appliances that are linked to perform as a single virtual appliance in an HA (high availability) configuration. The HA configuration provides hardware redundancy to minimize service outages. In this configuration, one appliance is the active node and the other is the passive node.</td>
</tr>
<tr>
<td>Host Record</td>
<td>On Infoblox appliances, host records provide a unique approach that enables you to manage multiple DNS records and DHCP and IPAM data collectively, as one object on the appliance.</td>
</tr>
<tr>
<td>IBOS (Infoblox Orchestration Server)</td>
<td>IBOS is the Infoblox IF-MAP (Interface to Metadata Access Points) server that contains a searchable database for storing state information about network resources. It is the central point with which IF-MAP clients communicate to send and retrieve real-time information defined in the IF-MAP data format.</td>
</tr>
<tr>
<td>IF-MAP (Interface for Metadata Access Points)</td>
<td>An open standard client-server protocol developed by the Trusted Computing Group as one of the core protocols of the TNC (Trusted Network Connect) open architecture. IF-MAP allows network resources to share real-time information.</td>
</tr>
<tr>
<td>IP Map</td>
<td>In Infoblox Grid Manager or System Manager, this is a graphical representation of all IPv4 addresses in a given subnet.</td>
</tr>
<tr>
<td>IPAM (IP Address Management)</td>
<td>Infoblox IPAM provides a means of planning, tracking, and managing IP address space in a network. It glues DNS and DHCP services together so that each service is aware of changes in the other. The Infoblox IPAM implementation offers an IP address-centric approach so you can manage your networks and IP addresses through a centralized GUI.</td>
</tr>
<tr>
<td>Leaf Network</td>
<td>On Infoblox appliances, a network that does not contain any subnets. Lease Logging Member An Infoblox Grid member that is designated to collect DHCP lease events.</td>
</tr>
</tbody>
</table>

Copyright ©2019, Infoblox, Inc. All right reserved.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Pool</td>
<td>A license pool is a container associated with the Grid and holds dynamic licenses for a specific feature. Licenses in the pool can be dynamically allocated to and deallocated from Grid members. When not in use, dynamic licenses are released back to the pool for future allocation. There is no expiration for dynamic licenses.</td>
</tr>
<tr>
<td>Limited-Access User</td>
<td>An admin user account that has specific roles and permissions assigned. Limited-access users have restricted access to Infoblox Multi-Grid Manager, Grid Manager, and System Manager, and can only perform certain tasks based on their assigned roles and permissions.</td>
</tr>
<tr>
<td>Lite Upgrade</td>
<td>On Infoblox appliances, a lite upgrade occurs when there are incremental changes to the NIOS software that do not require any change to the database. The appliance can perform a lite upgrade only if the format of the database between the existing NIOS version and the upgrade version is the same. In general, when you upgrade from a major release to a patch release or a patch release to another patch release, you are performing a lite upgrade.</td>
</tr>
<tr>
<td>Loopback Interface</td>
<td>On Infoblox appliances, the virtual network interface on which you can consolidate DNS servers for migration purposes, add anycast addresses to improve the performance of the DNS service, and separate DNS traffic.</td>
</tr>
<tr>
<td>Managing Member</td>
<td>An Infoblox Grid member that is configured to manage Microsoft DNS and DHCP servers.</td>
</tr>
<tr>
<td>Master Candidate</td>
<td>An Infoblox Grid member that is designated to assume the role of the Grid Master as a disaster recovery measure.</td>
</tr>
<tr>
<td>Master Grid</td>
<td>A group of Infoblox appliances that are connected to provide a single point of administration for multiple Grids and network management of these Grids.</td>
</tr>
<tr>
<td>Master Grid Member</td>
<td>Any single Infoblox appliance or HA pair that belongs to the Master Grid. All Master Grid members serve as Master Candidates.</td>
</tr>
<tr>
<td>Multi-Grid Manager</td>
<td>The NIOS web interface that provides access to the Master Grid, from which you can manage multiple Grids and their networks.</td>
</tr>
<tr>
<td>Multi-Grid Master</td>
<td>The Infoblox Master Grid member that maintains the NIOS database that is distributed among all Master Grid members. You connect to Multi-Grid Manager to configure and monitor the Master Grid.</td>
</tr>
<tr>
<td>Multi-Grid Master Candidate</td>
<td>An Infoblox Master Grid member that is designated to assume the role of the Multi-Grid Master as a disaster recovery measure.</td>
</tr>
<tr>
<td>Name Server Group</td>
<td>On Infoblox appliances, a server group that contains one primary DNS server and/or one or more secondary DNS servers. Specifying a single name server group can simplify DNS zone creation.</td>
</tr>
<tr>
<td>NAT (Network Address Translation) Group</td>
<td>A group of Infoblox Grid members that are configured on the same side of a NAT appliance. In a Grid configuration where the Grid Master is configured behind a NAT appliance and there are Grid members on both sides of the NAT appliance, it is necessary to create a NAT group to ensure that the Grid Master and Grid members use the correct NAT and interface addresses for Grid communications.</td>
</tr>
<tr>
<td>Network Block</td>
<td>On Infoblox appliances, an IP address space that is defined in the Master Grid. A network block can consist of other network blocks, network containers, and leaf networks.</td>
</tr>
<tr>
<td>Network Container</td>
<td>On Infoblox appliances, an automatically created container of multiple networks that are subnets of the IP address space configured for the network container. A network container cannot be assigned to a Grid member or be directly created.</td>
</tr>
<tr>
<td>Network Discovery</td>
<td>A set of tools provided by the Infoblox NIOS appliance for detecting active hosts on specified networks and specified VMware vSphere servers.</td>
</tr>
<tr>
<td><strong>Network Map</strong></td>
<td>In Infoblox Grid Manager and System Manager, Network Map presents a complete view of your network space, including the different types of networks that are in it and its unused address space. You can use Network Map to design and plan your network infrastructure, configure and manage individual networks, and evaluate their utilization.</td>
</tr>
<tr>
<td><strong>Network Mask or Netmask</strong></td>
<td>A numeric representation of the bits that are used to split an IP address into the network portion and the host portion. In Infoblox products, this is represented by either quad-dotted decimal representation or CIDR notation for IPv4 network masks, or by CIDR notation for IPv6 network masks.</td>
</tr>
<tr>
<td><strong>Network View</strong></td>
<td>On Infoblox appliances, a single routing domain with its own networks and shared networks. A network view can contain both IPv4 and IPv6 networks. All networks must belong to a network view on the Infoblox appliance.</td>
</tr>
<tr>
<td><strong>NIOS</strong></td>
<td>An Infoblox proprietary system that powers Infoblox solutions with an embedded processor that delivers core network services. It is the operating system that runs on the NIOS appliances—a security-hardened, real-time set of appliances built to ensure the non-stop operation of network infrastructure. NIOS automates the error-prone and time-consuming manual tasks associated with deploying and managing IPAM, DNS, and DHCP required for continuous IP network availability and business uptime.</td>
</tr>
<tr>
<td><strong>NIOS Virtual Appliance</strong></td>
<td>Any Infoblox supported platform, such as the Riverbed Steelhead appliances or VMWare appliances, that runs the vNIOS software. These appliances are also known as the vNIOS appliances.</td>
</tr>
<tr>
<td><strong>Node</strong></td>
<td>A single Infoblox appliance of an HA (high availability) pair. An HA pair consists of an active node and a passive node.</td>
</tr>
<tr>
<td><strong>NTP (Network Time Protocol)</strong></td>
<td>A protocol for synchronizing the clocks of computer systems over packet-switched, variable latency data networks; it essentially keeps network devices on a common clock by resisting the effects of variable latency by means of a jitter buffer.</td>
</tr>
<tr>
<td><strong>Passive Node</strong></td>
<td>The Infoblox NIOS appliance in an HA pair that constantly keeps its database synchronized with that of the active node, so it can take over core network services when an HA failover occurs. When an HA failover occurs, the passive node becomes the active node in the HA pair.</td>
</tr>
<tr>
<td><strong>PortIQ</strong></td>
<td>An Infoblox switch port appliance that enables quick discovery of the Ethernet switch ports. PortIQ identifies ports that are not fully utilized and those that exceed their capacity. You can use PortIQ to troubleshoot LAN environments.</td>
</tr>
<tr>
<td><strong>Quick Filter</strong></td>
<td>A filter that stores specific filter criteria for requesting information displayed in a specific panel in Infoblox Multi-Grid Manager, Grid Manager, and System Manager. For more information, see &quot;Filter.&quot;</td>
</tr>
<tr>
<td><strong>Overlapping Network</strong></td>
<td>On Infoblox appliances, a network that exists in multiple locations, which can be multiple Grids in the Master Grid or within various network views in a Grid.</td>
</tr>
<tr>
<td><strong>Replication</strong></td>
<td>Database distribution among the Infoblox Grid Master and Grid members as well as among the Multi-Grid Master and Master Grid members.</td>
</tr>
<tr>
<td><strong>Replication Factor (Reporting - Multi-Site Cluster)</strong></td>
<td>The number of copies of reporting data in each bucket that the cluster maintains.</td>
</tr>
<tr>
<td><strong>Reservation</strong></td>
<td>On Infoblox appliances, a static IP address that you create for future use. A reservation is a pre-provisioned fixed address. You can reserve this static IP address on the NIOS appliance and assign it to a client in the future.</td>
</tr>
<tr>
<td><strong>Resource Records</strong></td>
<td>A collection of data in the DNS server database. Each resource record specifies information about a DNS object. For example, an A (address mapping) record maps a host name to an IP address, and a PTR (reverse-lookup pointer) record maps an IP address to a host name. The DNS server uses these records to answer queries.</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Roaming Host</strong></td>
<td>On Infoblox appliances, a host with a dynamically assigned IP address and a specific set of properties and DHCP options. When you create a roaming host for a network device, the device can receive any dynamically assigned address from the network to which it belongs.</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>A DHCP address range on a Microsoft server. Microsoft scope information is converted to equivalent DHCP range information after Microsoft data is synchronized with the NIOS appliance.</td>
</tr>
<tr>
<td><strong>Search Factor</strong></td>
<td>The number of searchable copies of reporting data in each bucket that the cluster maintains.</td>
</tr>
<tr>
<td><strong>Shared Network</strong></td>
<td>On Infoblox appliances, a network segment to which you assign two or more subnets. When subnets in a shared network contain IP addresses that are available for dynamic allocation, the addresses are put into a common pool for allocation when client requests arise.</td>
</tr>
<tr>
<td><strong>Shared Record Group</strong></td>
<td>On Infoblox appliances, a set of resource records that you add to multiple DNS zones. You can create resource records in a group and share the group among multiple zones. The zones handle the shared resource records as any other resource record.</td>
</tr>
<tr>
<td><strong>SSO (Single Sign On)</strong></td>
<td>An Infoblox feature that allows you to automatically sign in to selected Grids from the Master Grid, without having to log in to each individual Grid each time you sign on.</td>
</tr>
<tr>
<td><strong>Smart Folder</strong></td>
<td>On Infoblox appliances, a virtual folder in which you place the results of filter criteria that you select to request specific data in the NIOS database. Once you set up a smart folder, the appliance displays up-to-date information based on your filter and grouping criteria each time you access the folder.</td>
</tr>
<tr>
<td><strong>Subnet (or network)</strong></td>
<td>A logical division of an IP network. A subnet of network may also be called a network. For example, 10.1.0.0/16 is a subnet of 10.0.0.0/8, and fc80:8:8:16::/64 is a subnet of fc80:8:8::/48.</td>
</tr>
<tr>
<td><strong>Superscope</strong></td>
<td>On a Microsoft server, superscope comprises multiple scopes or DHCP address ranges created on a single physical network segment. Microsoft superscope information is converted to equivalent network information after Microsoft data is synchronized with the NIOS appliance.</td>
</tr>
<tr>
<td><strong>Superuser</strong></td>
<td>An admin user account that has unrestricted access to Infoblox Multi-Grid Manager, Grid Manager, or System Manager.</td>
</tr>
<tr>
<td><strong>Support Bundle</strong></td>
<td>A tar.gz file that contains configuration files and system files of the Infoblox NIOS appliance. You can download a support bundle for an independent appliance and for each member in a Grid.</td>
</tr>
<tr>
<td><strong>System Manager</strong></td>
<td>The NIOS web interface that provides access to an independent appliance (single or HA) for performing IPAM, DNS, and DHCP management and other administration tasks.</td>
</tr>
<tr>
<td><strong>TFTP (Trivial File Transfer Protocol)</strong></td>
<td>A data transfer service that provides devices—such as phones, RFID readers, IP cameras, and other devices—with up-to-date software and configuration data.</td>
</tr>
<tr>
<td><strong>Traffic Capture</strong></td>
<td>An Infoblox tools that captures the traffic on one or all of the ports on a NIOS appliance. The NIOS appliance saves all captured traffic in a .cap file and compresses it into a .tar.gz file.</td>
</tr>
<tr>
<td><strong>Upgrade Group</strong></td>
<td>On Infoblox appliances, a group of Grid members that you put together so you can perform software distribution and upgrade at the same time.</td>
</tr>
</tbody>
</table>
VIP (Virtual IP) | On Infoblox appliances, the shared IP address of an HA pair. A VIP address links to the HA port on the active node of an HA pair.
VRID (Virtual Router ID) | VRID identifies the VRRP (Virtual Router Redundancy Protocol) HA pair to which the Infoblox appliance belongs. Through VRID, two HA nodes identify each other as belonging to the same HA pair, and they obtain a virtual MAC address to share with a VIP. A VRID can be any number between 1 and 255, and it must be unique on the local LAN so that it does not conflict with any other Infoblox appliances using VRRP on the same subnet.
vNIOS | The virtual version of NIOS. You can install Infoblox vNIOS software on any supported virtual platform and configure the system as a vNIOS virtual appliance.
VRRP (Virtual Router Redundancy Protocol) | An industry standard MAC address level HA failover mechanism.

Appendix B Grid Manager Icons

This appendix contains the following information about icons used in Grid Manager, System Manager, and Orchestration Server Manager:

- **Icon**: The graphical display of an icon.
- **Icon Name**: The icon name.
- **Description**: The task that Grid Manager performs after you click the icon.
- **Tab/Table/Panel**: Lists the tab, table, or panel in which the icon appears.

The following are common icons that appear in most of the tabs, tables, and panels, and in the Toolbar:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Active User</td>
<td>Indicates a user is active on the Microsoft server.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Add</td>
<td>Adds an object</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Add Bookmark</td>
<td>Adds a bookmark for an object and displays it in the Bookmarks panel</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Arrow (Down)</td>
<td>Moves an object down in a list</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Arrow (Up)</td>
<td>Moves an object up in a list</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Clear</td>
<td>Clears the status of an object</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Clock</td>
<td>Displays a drop-down list for time</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Delete</td>
<td>Deletes an object</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Disabled</td>
<td>Indicates a disabled object</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Download</td>
<td>Downloads a file or data</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Edit</td>
<td>Displays the corresponding editor for modifying object configurations</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Edit</td>
<td>Displays the corresponding editor for modifying object configurations</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Execute Now</td>
<td>Executes a scheduled task immediately</td>
<td></td>
</tr>
<tr>
<td>Export</td>
<td>Exports data in the current panel</td>
<td></td>
</tr>
<tr>
<td>Extensible Attribute</td>
<td>Configures extensible attributes for the selected object</td>
<td></td>
</tr>
<tr>
<td>Flat View</td>
<td>Displays a list of objects in a flat view</td>
<td></td>
</tr>
<tr>
<td>Help</td>
<td>Displays information about an object</td>
<td></td>
</tr>
<tr>
<td>Hierarchy</td>
<td>Displays objects in a hierarchical view</td>
<td></td>
</tr>
<tr>
<td>Indexer</td>
<td>Indicates that the reporting member functions as an indexer.</td>
<td></td>
</tr>
<tr>
<td>Import</td>
<td>Imports a file or data</td>
<td></td>
</tr>
<tr>
<td>Import Job Manager</td>
<td>Imports CSV data</td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>Displays informational data about an object</td>
<td></td>
</tr>
<tr>
<td>Locked</td>
<td>Indicates a locked object</td>
<td></td>
</tr>
<tr>
<td>Microsoft Server</td>
<td>Indicates a Microsoft server</td>
<td></td>
</tr>
<tr>
<td>Pause</td>
<td>Pauses a function</td>
<td></td>
</tr>
<tr>
<td>Print</td>
<td>Prints the information in the current panel</td>
<td></td>
</tr>
<tr>
<td>Restart/Processing</td>
<td>Restarts services on the appliances or indicates a request is in progress</td>
<td></td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes the current page or table</td>
<td></td>
</tr>
<tr>
<td>Report</td>
<td>Displays a report, such as the capacity report</td>
<td></td>
</tr>
<tr>
<td>Search</td>
<td>Searches for specific objects</td>
<td></td>
</tr>
<tr>
<td>Search Head</td>
<td>Indicates that the reporting member functions as a search head</td>
<td></td>
</tr>
<tr>
<td>Selected object</td>
<td>Selects an object in a table for a specific function</td>
<td></td>
</tr>
<tr>
<td>Start</td>
<td>Starts a process</td>
<td></td>
</tr>
<tr>
<td>Stop</td>
<td>Stops a process</td>
<td></td>
</tr>
<tr>
<td>Icon</td>
<td>Icon Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| ![Configure](image_url) | Configure                | • Configures DHCP properties  
• Configures File Distribution properties  
• Configures Licenses         | Data Management tab -> DHCP tab  
Data Management tab -> DHCP tab -> toolbar  
Data Management tab -> DHCP tab -> toolbar  
Grid tab -> Grid Manager tab -> toolbar |
<p>| <img src="image_url" alt="Conflict" /> | Conflict                  | Indicates an IP address conflict                                               | Data Management tab -&gt; IPAM tab -&gt; Net Map                                      |
| <img src="image_url" alt="Convert" />   | Convert                   | Converts an object                                                             | Data Management tab -&gt; IPAM tab -&gt; Net -&gt; IP Map -&gt; toolbar                     |
| <img src="image_url" alt="Discovery" /> | Discovery                 | Performs a network discovery                                                   | Data Management tab -&gt; IPAM tab -&gt; toolbar                                      |
| <img src="image_url" alt="Force HA Failover" /> | Force HA Failover | Forces an HA failover                                                         | Data Management tab -&gt; DHCP tab -&gt; toolbar                                      |
| <img src="image_url" alt="Force Recovery" /> | Force Recovery | Forces a recovery                                                              | Data Management tab -&gt; DHCP tab -&gt; Members tab -&gt; Failover Associations tab -&gt; toolbar |
| <img src="image_url" alt="Grid Manager" /> | Grid Manager              | Indicates the Grid Master                                                      | Data Management tab -&gt; DHCP tab -&gt; Members tab -&gt; toolbar                      |
| <img src="image_url" alt="Grid Manager Candidate" /> | Grid Manager Candidate | Indicates the Grid Master candidate                                            | Data Management tab -&gt; DHCP tab -&gt; Members tab -&gt; toolbar                      |
| <img src="image_url" alt="Grid Member" /> | Grid Member               | Indicates the Grid member                                                      | Data Management tab -&gt; DHCP tab -&gt; Members tab -&gt; toolbar                      |
| <img src="image_url" alt="Join" />       | Join                      | Joins networks                                                                | Data Management tab -&gt; IPAM tab -&gt; network -&gt; toolbar                          |
| <img src="image_url" alt="Key-signing Key Rollover" /> | Key-signing Key Rollover | Indicates the key-signing key that is due to rollover                          | Data Management tab -&gt; DNS tab                                                  |
| <img src="image_url" alt="Leaf Network" /> | Leaf Network              | Indicates a leaf network                                                       | Data Management tab -&gt; IPAM tab or DHCP tab                                     |
| <img src="image_url" alt="Disabled Leaf Network" /> | Disabled Leaf Network | Indicates a disabled leaf network                                               | Data Management tab -&gt; IPAM tab or DHCP tab                                     |
| <img src="image_url" alt="Microsoft Server" /> | Microsoft Server          | Indicates a Microsoft server                                                   | Data Management tab -&gt; DHCP tab -&gt; Members tab -&gt; toolbar                      |
| <img src="image_url" alt="Multi-Ping" /> | Multi-Ping                | Pings all the addresses in a network                                           | Data Management tab -&gt; IPAM tab -&gt; IP Map -&gt; toolbar                           |</p>
<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Description</th>
<th>Tab/Table/Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Container</td>
<td>Indicates a non-cloud network container</td>
<td>Data Management tab -&gt; IPAM tab or DHCP tab</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Indicates a non-cloud network</td>
<td>Data Management tab -&gt; IPAM tab or DHCP tab</td>
<td></td>
</tr>
<tr>
<td>Network Container (for Cloud platform appliance)</td>
<td>Indicates a <strong>cloud</strong> network container</td>
<td>Cloud tab -&gt; Networks tab or Data Management tab -&gt; IPAM tab or DHCP tab</td>
<td></td>
</tr>
<tr>
<td>Network (for Cloud platform appliance)</td>
<td>Indicates a <strong>cloud</strong> network</td>
<td>Cloud tab -&gt; Networks tab or Data Management tab -&gt; IPAM tab or DHCP tab</td>
<td></td>
</tr>
<tr>
<td>Network (Disabled)</td>
<td>Indicates a disabled network</td>
<td>Data Management tab -&gt; IPAM tab or DHCP tab</td>
<td></td>
</tr>
<tr>
<td>Microsoft Network</td>
<td>Indicates a network with Microsoft servers</td>
<td>Data Management tab -&gt; IPAM tab or DHCP tab</td>
<td></td>
</tr>
<tr>
<td>Infoblox Network</td>
<td>Indicates a network with Infoblox appliances</td>
<td>Data Management tab -&gt; IPAM tab or DHCP tab</td>
<td></td>
</tr>
<tr>
<td>Ping</td>
<td>Pings an IP address</td>
<td>Data Management tab -&gt; IPAM tab -&gt; IP Map -&gt; Toolbar</td>
<td></td>
</tr>
<tr>
<td>Properties</td>
<td>Configures Grid DNS properties</td>
<td>Data Management tab -&gt; DNS tab -&gt; Toolbar</td>
<td></td>
</tr>
<tr>
<td>Reclaim</td>
<td>Reclaims an IP address</td>
<td>Data Management tab -&gt; IPAM tab -&gt; IP Map -&gt; Toolbar</td>
<td></td>
</tr>
<tr>
<td>Resize</td>
<td>Resizes a network</td>
<td>Data Management tab -&gt; IPAM tab -&gt; network -&gt; Toolbar</td>
<td></td>
</tr>
<tr>
<td>Resolve Conflict</td>
<td>Resolves an IP address conflict</td>
<td>Data Management tab -&gt; IPAM tab -&gt; IP Map -&gt; Toolbar</td>
<td></td>
</tr>
<tr>
<td>Set Partner Down</td>
<td>Sets partner down</td>
<td>Data Management tab -&gt; DHCP tab -&gt; Members tab -&gt; Failover Associations tab -&gt; Toolbar</td>
<td></td>
</tr>
<tr>
<td>Split Network</td>
<td>Splits a network</td>
<td>Data Management tab -&gt; IPAM tab -&gt; network -&gt; Toolbar</td>
<td></td>
</tr>
<tr>
<td>DNSSEC status</td>
<td>Displays status for DNSSEC</td>
<td>Data Management tab -&gt; DNS tab -&gt; Toolbar</td>
<td></td>
</tr>
<tr>
<td>Secondary Zone Status</td>
<td>Displays status for the secondary zone</td>
<td>Data Management tab -&gt; DNS tab</td>
<td></td>
</tr>
<tr>
<td>Zoom In</td>
<td>Zooms in to the selected network</td>
<td>Data Management tab -&gt; IPAM tab -&gt; Net Map</td>
<td></td>
</tr>
<tr>
<td>Zoom Out</td>
<td>Zooms out from the selected network</td>
<td>Data Management tab -&gt; IPAM tab -&gt; Net Map</td>
<td></td>
</tr>
<tr>
<td>Directory</td>
<td>Indicates a directory</td>
<td>Data Management tab -&gt; File Distribution tab</td>
<td></td>
</tr>
</tbody>
</table>

The following icons appear in the **Smart Folders** tab:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
<th>Tab/Table/Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Folder</td>
<td>Lists a smart folder</td>
<td>Smart Folders tab</td>
<td></td>
</tr>
<tr>
<td>Smart Folder (Group By)</td>
<td>Lists smart folders in a group-by list</td>
<td>Smart Folders tab</td>
<td></td>
</tr>
<tr>
<td>Smart Folder (Link)</td>
<td>Indicates a link to the smart folder</td>
<td>Smart Folders tab and other selectors</td>
<td></td>
</tr>
</tbody>
</table>

The following icons appear in the **Grid** tab:
Backup | Backs up the configuration file and database | Grid tab -> Grid Manager tab -> Toolbar
---|---|---
Restore | Restores the configuration file and database | Grid tab -> Grid Manager tab -> Toolbar
bloxTools | Performs bloxTools services | Grid tab -> Grid Manager tab -> Toolbar
Certificate | Creates, generates, uploads, or downloads an HTTPS certificate | Grid tab -> Grid Manager tab -> Toolbar
Control | Restarts, reboots, or shuts down a member | Grid tab -> Grid Manager tab -> Members tab -> member -> Toolbar
Manage Services | Manages member services | Grid tab -> Grid Manager tab -> Members tab -> member
Syslog | Displays the syslog file | Grid tab -> Grid Manager tab -> Members tab -> member -> Toolbar
Traffic Capture | Captures the traffic report on a member | Grid tab -> Grid Manager tab -> Members tab -> member -> Toolbar

The following icons appear in the Administration tab:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
<th>Tab/Table/Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute Now</td>
<td>Executes a scheduled task immediately</td>
<td>Administration tab -&gt; Scheduling tab -&gt; Toolbar</td>
<td></td>
</tr>
<tr>
<td>Overlap</td>
<td>Shows overlapping permissions</td>
<td>Administration tab -&gt; Permissions tab</td>
<td></td>
</tr>
<tr>
<td>Reschedule</td>
<td>Reschedules a task</td>
<td>Reschedules a task Administration tab -&gt; Scheduling tab -&gt; Toolbar</td>
<td></td>
</tr>
<tr>
<td>Schedule Delete</td>
<td>Schedules a deletion for a task</td>
<td>Administration tab -&gt; Scheduling tab -&gt; Toolbar</td>
<td></td>
</tr>
</tbody>
</table>

The following icons appear in the Finder panel:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bookmarks</td>
<td>Lists all bookmarked objects</td>
<td></td>
</tr>
<tr>
<td>Recycle Bin</td>
<td>Lists all deleted objects</td>
<td></td>
</tr>
<tr>
<td>Smart Folders</td>
<td>Lists all smart folders</td>
<td></td>
</tr>
<tr>
<td>URL Links</td>
<td>Adds URL links</td>
<td></td>
</tr>
</tbody>
</table>

The following icons appear in the Load Balancer related panels:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Icon Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Management Visualizer</td>
<td>Views GLB object map</td>
<td></td>
</tr>
<tr>
<td>DNS View Mapping</td>
<td>Maps NIOS DNS view to GLB DNS view</td>
<td></td>
</tr>
</tbody>
</table>

The following icons appear in Multi-Grid Manager:
Appendix C Guidance Documentation Supplement for Common Criteria

Common Criteria provides an independent and objective evaluation of the security of Information Technology (IT) products. It gives assurance that the product satisfies a set of internationally recognized security standards.

This document provides additional guidance on the secure installation of the Target of Evaluation (TOE) for Common Criteria Evaluation Assurance Level (EAL) 2 Augmented ALC_FLR.2. For more information about the Common Criteria mode, refer to the following:

https://www.commoncriteriaportal.org/
https://www.commoncriteriaportal.org/files/epfiles/Infoblox%20Appliances%20with%20NIOS%20v8.2.6%20ST%20v1.0.pdf
https://www.commoncriteriaportal.org/files/epfiles/Infoblox%20Appliances%20with%20NIOS%20v8.2.6%20ST%20v1.1.pdf

The TOE includes the following Infoblox appliances: IB-825, IB-1425, IB-2225, IB-4015, IB-4025, IB-V825, IB-V1425, IB-V2225, IB-V4015, and IB-V4025 with NIOS version 8.2.6, which are network appliances that provide delivery of IP network services and management, Grid and HA configuration. The TOE is a network device that consolidates the delivery and management of core IP network services including DNS, DHCP, IPAM, FTP, TFTP and HTTP. These appliances can be made compliant with Common Criteria and FIPS 140-2 security standards. When you enable the Common Criteria mode, only the respective mode is enabled in the device. If you enable FIPS mode on the device, it enables both Common Criteria and FIPS modes. For more information about FIPS mode, see Guidance Documentation Supplement for Federal Information Processing Standard.

To ensure that your appliance is Common Criteria compliant, make sure that your hardware and software settings match the evaluated configuration that was certified for Common Criteria.

This document provides clarifications and changes to the Infoblox Administrator Guide and Infoblox CLI Guide, and should be used as the guiding document for installation of the TOE in the Common Criteria evaluated configuration.

This appendix contains the following sections:

- Pre-Requisites
- Verifying the Hardware
- Security Guidelines
- Installation and Configuration
- Administration
  - Setting Password Restrictions for Local Admins
- Enabling/Disabling Common Criteria Mode
  - Using the CLI
- Licenses and Services
- WebUI Settings
  - Creating a Login Banner
  - Modifying the Session Timeout Setting
  - Managing Certificates
- Backing Up and Restoring the Database
- Secure Syslog Transport
- Audit Log
- Syslog

**Pre-Requisites**

Before you begin the configuration, ensure that you have all the necessary components. The following are needed and must be acquired before continuing with this guidance:

1. One of the following supported Infoblox appliance models: IB-825, IB-1425, IB-2225, IB-4015, IB-4025, IB-V825, IB-V1425, IB-V2225, IB-V4015, and IB-V4025 running NIOS version 8.2.
2. A management station or computer from which you configure and manage the NIOS appliance. See Management System Requirements for the system and browser requirements.
Verifying the Hardware

To verify the secure delivery of the hardware:

- Use the tracking number of the order to review the status of the shipment.
- Inspect the tamper-evident seals for any signs of tampering.
- Verify the product by comparing the shipping slip with the invoice.

Security Guidelines

Following are security assumptions to ensure that the TOE is administered in a secure manner after it is delivered:

- The environment ensures the physical security of the TOE, commensurate with its value and the value of the data that it contains.
- Administrators are non-hostile, properly trained and trusted to apply all administrator guidance.
- Administrators will take appropriate measures to prevent unauthorized individuals from accessing the TOE.

Note the following:

- When you configure a Grid Master and enable a certain, either CC or FIPS, mode in the Grid Master and then configure a Grid member with a different mode than that of the Grid Master, the member automatically takes the same mode as the Grid Master when you add this member to the Grid Master. For example, if the Grid Master is in FIPS mode and the Grid member is CC mode enabled, the Grid member becomes FIPS enabled when you add this member to the Grid.
- Consider an HA Grid Master with a certain, either CC or FIPS, mode enabled in the active node. When you join a passive node to the HA Grid Master, it automatically takes the same mode as the Grid Master in the active node. For example, if FIPS is enabled in the active node, then the passive node too becomes FIPS enabled when you join it to the HA Grid Master even though it was in CC mode earlier.
- When the HA pair is enabled, you cannot enable or disable either the CC or FIPS mode on the active or passive nodes.

Infoblox suggests that you do the following for an HA pair:

- Set either CC or FIPS mode on each node before building an HA pair.
- Set both the nodes of an HA pair in the same mode, that is either in the CC mode, or FIPS mode, or none.

Installation and Configuration

To ensure the security of the installation and configuration of the TOE:

- Administrators must install the appliance according to the procedures in the installation guides.
- The TOE contains an option for upgrading the system. This is available only for security administrators. The security administrator will be able to upgrade to a validated release package only. The security administrator can verify the TOE by the version number included in the file name as well as through the administrative interface before and after the upgrade. When upgrading, ensure that the .bin2 file is uploaded, and not the .bin file. Refer to the Release Notes of the NIOS version to which the TOE is upgrading for additional upgrade instructions.
- Users’ access to the TOE is controlled by security mechanisms and unauthorized users are denied access to the TOE. For more information, see Administration.
- The TOE provides external authentication mechanisms for remote users using SSL with Active Directory. For more information, see Authenticating Admins Using Active Directory.

Secure Delivery of NIOS Virtual Software Package

You can download the NIOS virtual software from the Infoblox Technical Support site. To download the software, you must have a valid login account on the Infoblox Support site. Register your product at https://support.infoblox.com if you do not already have an account. This software package consists of a template file with .ova extension for all the supported NIOS appliance models. Make sure that you download the file with an extension that corresponds to the appliance model number. You can deploy the NIOS virtual appliance from a remote web server or a local file system accessible from your management system. To verify the version of the software that you are running, you can use the show version command.

You can validate the file downloaded from the Infoblox support website using the MD5/SHA256/SHA512 checksum provided on the support portal at https://support.infoblox.com. To verify the checksum, you can execute the md5sum/sha256sum/sha512sum command from the Unix/Linux based system or use Cygwin installed on a Windows machine. In addition, there are paid and freeware versions that you can install and execute from Windows. For a Mac OS, you can use the md5/shasum -a 256/shasum -a 512 command. Infoblox recommends that you use what is appropriate for your environment.

The Infoblox appliance ships with a default user name and password. Change the default admin account password immediately after the system is installed to safeguard its use. Make sure that the NIOS appliance has at least one administrator account with superuser privileges at all times, and keep a record of your account information in a safe place. You can create new administrator accounts, with or without superuser privileges. For more information, see Managing Administrators.

The Common Criteria compliant hardware platform that hosts NIOS virtual is VMware ESXi, either version 5.5 or 6.5, with the following system hardware:

- HP DL380 G9 host platform
- Intel Xeon Family processor E5-2680v3 CPU

Copyright ©2019, Infoblox, Inc. All right reserved.
• 128GB RAM (8 x HP 752369)

Administration

A user must have an admin account to log in to the TOE. Each admin account belongs to an admin group, which contains roles and permissions that determine the tasks a user can perform. The TOE provides a default superuser admin group, called admin-group, with one superuser administrator, admin. The default superuser admin can log in to the TOE, using the default user name admin and password infoblox. Superuser admins are the security admins and have full access and control of all the operations of a TOE. Note that you must change the default user name and password of the default superuser admin to prevent unauthorized access to the TOE. Only superusers can do the following:

• Create admin accounts and groups. For more information, see Chapter 4, Managing Administrators.
• Set password parameters. For more information, see Managing Passwords.
• Create the login banner. For more information, see Creating a Login Banner.
• Set the session timeout. For more information, see Modifying the Session Timeout Setting.
• Manage authentication policy. For more information, see About Remote Admins.
• Manage TOE system time. For more information, see Managing TOE System Time.

Limited-access admin groups provide their members with read-only or read/write access to specific resources such as Grid member, DNS, and DHCP. These admin groups can access the appliance through the remote console, GUI, API, or both. When you provide write access to all Grid members, the TOE allows Grid members to configure audit records to display a detailed or a brief summary. Infoblox recommends that you add only pre-defined roles to the admin groups from the TOE. In addition, limited-access admins are not allowed to perform the following tasks:

• Download the support bundle.
• Enable SNMP on the appliance.
• Upload files that are larger than 100 MB. If the file size is greater than the maximum size allowed, the Upload dialog box closes and an error message is displayed in the feedback panel. The attempt to upload a file that exceeded the maximum will be logged to syslog. Non-superusers only are able to upload files for file distribution and do CSV import.
• Manage audit configuration.

Setting Password Restrictions for Local Admins

All admins are required to enter a username and password when they log in to Grid Manager or the CLI. The password is always obscured when an admin logs in. The TOE defaults to locking out the user after three consecutive failed logins. A superuser must define a password policy that is consistent with the security policy of the organization. The password policy specifies the minimum password length and character types, such as lowercase or uppercase characters, that are allowed in the password. In addition, the policy specifies the number of required character changes from the previous password, whether passwords expire and their duration. Additionally, you can require admins to change their passwords when they first log in or after their passwords are reset. For information about defining the password policy, see Managing Passwords. Local admins must change their passwords according to the defined password policy. A password can be changed as follows:

• By the local admin in the User Profile page. For more information, see Changing the Password and Email Address.
• By the local admin when a password expires or when the admin first logs in. Note that this applies to logging in to the CLI or WebUI.
• By a superuser admin.

Managing TOE System Time

You can manually set the date and time for a TOE or enable NTP. You cannot manually configure the date and time when NTP service is enabled. Changing the date and time resets the application and terminates the management session. For information about setting the system time, see Managing Time Settings.

Enabling / Disabling Common Criteria Mode

**Note:** Infoblox recommends that you do not change the Common Criteria setting of a NIOS appliance that is in a production environment.

Before you enable Common Criteria mode, you must reset a NIOS appliance to its original factory settings. This removes the database, network settings, logs, and configuration files. Then, it reboots with its factory settings, which are the default user name and password, and default network settings. If you do not reset the appliance to its original factory settings, the appliance will not be Common Criteria compliant, even if you enable Common Criteria mode.

To reset the NIOS appliance to its factory settings:
1. Log in to the Infoblox CLI using a superuser account.
2. Enter the following CLI command:

   ```
   reset all
   ```

You can enable and disable Common Criteria mode from the Infoblox CLI only. Do the following to set Common Criteria mode on the appliance:

1. Log in to the Infoblox CLI. After executing the `reset all` command, you can log in to the TOE only by using the default superuser admin name admin and password infoblox.
2. Type the following command:

   `set cc_mode`

For more information about the commands mentioned above, refer to the *Infoblox CLI Guide*. The TOE reboots and goes through boot time self tests. If the test fails, the TOE goes into a loop and displays an error message on the serial console and the LCD. Otherwise, it displays the Login prompt after the self tests.

**Note:** You cannot enable the Common Criteria mode when the FIPS mode is enabled, but note that Common Criteria mode is a subset of the FIPS mode. When you enable FIPS mode in your device, it enables both FIPS and Common Criteria mode. For more information about the FIPS mode, see Appendix D Guidance Documentation Supplement for Federal Information Processing Standard.

To clear Common Criteria mode on an appliance, log in to the Infoblox CLI and execute the command: `reset all`.

### Using the CLI

Only superusers can access the CLI. You can access the CLI through a direct console or using the SSH command in Common Criteria or FIPS mode and also activate the option *Enable Remote Console Access* in the Grid or Member Properties editor.

To access the Infoblox CLI through the console port:

1. Connect a serial cable from the console port on your management system to the console port on the appliance. The appliance has a male DB-9 console port on its front panel.
2. Use the following connection settings to launch an emulation session through a serial terminal emulation program such as Hilgraeve Hyperterminal® (provided with the Windows® operating systems):
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: Xon/Xoff
3. Use the following default user name and password to log in to the Infoblox appliance:
   
   ```
   admin
   infoblox
   ```

   **Note:** After you log in, change the default user name and password of the default superuser admin to prevent unauthorized access to the TOE. For more information on changing passwords, see *Changing the Password and Email Address*. You can remotely (SSH) log in to the Grid Master candidate and execute the commands.

For more information about the Infoblox CLI, refer to the *Infoblox CLI Guide*.

### Licenses and Services

The TOE does not have general computing capabilities, other than the services required for the operation, administration and support of the TOE. In the evaluated configuration, the TOE has only the following licenses installed: NIOS, Grid, DNS, DHCP, Microsoft Management, DNS Cache Acceleration, Multi-Grid Management, Remote authentication using RADIUS and TACACS+, and Query Redirection. It also supports HSM (Hardware Security Module) Signing, and Remote Console Access. For more information about licenses, see *Managing Licenses*. You can access the remote console using the SSH command. Infoblox also supports SNMPv3 in the Common Criteria mode. The following services are disabled by default in the Common Criteria evaluated configuration and no claims are made regarding their function:

- `bloxTools`
- `Support access`

Installing additional licenses or enabling any of the listed services may result in a non-compliant system.

### WebUI Settings

This section describes the properties that you can set to ensure the security of the Grid Manager web interface.

#### Creating a Login Banner

Before establishing a user session via the WebUI, the TOE displays an initial banner regarding unauthorized use. The message is displayed before the session is established. You can change this message to your organization’s specific advisory notice and warning message regarding unauthorized use of the system. For information about defining the login banner, see *Creating a Login Banner*.

#### Modifying the Session Timeout Setting

You can set the length of idle time before an administrative session to the WebUI times out. The default timeout value is 600 seconds (10 minutes). If an admin does not interact with the application for the specified time, the TOE displays a message that a timeout has occurred. The
admin is then required to log back in to Grid Manager. For information about setting the session timeout, see \textit{Modifying the Session Timeout Setting}.

\section*{Managing Certificates}

The TOE generates a self-signed certificate when it first starts. Because the default certificate is self-signed, your browser does not have a trusted CA certificate or a cached NIOS appliance server certificate (saved from an earlier connection) to authenticate the NIOS appliance certificate. Also, the hostname in the default certificate is www.infoblox.com, which is unlikely to match the hostname of your NIOS appliance. Consequently, a message appears warning that the certificate is not from a trusted certifying authority and that the hostname on the certificate is either invalid or does not match the name of the site that sent the certificate. To eliminate certificate warnings, you can replace the default self-signed certificate with a different certificate.

After the initial login, you can do one of the following:

\begin{itemize}
  \item Generate another self-signed certificate with the correct hostname and save it to the certificate store of your browser.
  \item Request a CA-signed certificate with the correct hostname by generating a Certificate Signing Request (CSR) and sending it to your trusted Certificate Authority (CA). Then when you receive the certificate from the CA, import it to the appliance.
\end{itemize}

For information about these tasks, see \textit{Managing Certificates}.

For Common Criteria compliance, superusers must not use CSRs or certificates with keys smaller than 2048 bits. Limited access users are not allowed to upload a certificate with a key that is smaller than 2048 bits, or create a certificate signing request or self-signed certificate with a key size that is smaller than 2048 bits.

\section*{Backing Up and Restoring the Database}

You must log in with a superuser account to back up files. The administrator must back up system files to the local appliance. You can restore a backup file to an appliance running the same NIOS version as that of the appliance from which the backup file originates. You can also restore a backup file from an appliance running a NIOS version to an appliance running a later NIOS version as long as the upgrade from the earlier NIOS version to the later version is supported. Note that if you need to restore a backup file to an appliance, ensure that the backup file that you are restoring is from an appliance that was Common Criteria compliant as well.

For more information about backing up and restoring the database, see \textit{Backing Up and Restoring Configuration Files}.

\section*{Secure Syslog Transport}

The TOE provides the secure syslog transport feature using the TLS protocol. This allows secure transmission of messages between the syslog client, i.e. your NIOS appliance, and an external syslog server. You must use this feature to be Common Criteria compliant. To ensure secure syslog transport, you add a trusted CA certificate of the server to your NIOS appliance. The certificate is then used to establish a secure connection to the server before transmitting data. For more information, see \textit{Specifying Syslog Servers}.

\section*{SSL and TLS Protocols}

You can enable SSL and TLS protocols in CC mode using the following commands:

\begin{itemize}
  \item \texttt{set ssl_tls_settings}: Use this command to override or restore the default SSL/TLS settings.
  \item \texttt{set ssl_tls_protocols}: Use this command to enable or disable the SSL/TLS protocols.
  \item \texttt{set ssl_tls_ciphers}: Use this command to enable or disable the SSL/TLS cipher suites.
\end{itemize}

For more information about the SSL/TLS protocols, see \textit{SSL and TLS Protocols}. For more information about the list of commands related to SSL/TLS protocols and ciphers, refer to the \textit{Infoblox CLI Guide}.

The commands listed below display the default settings of SSL/TLS protocols in CC mode:

\begin{verbatim}
Infoblox > show ssl_tls_protocols
TLSv1.0  TLSv1.1  TLSv1.2
Infoblox > show ssl_tls_ciphers
TLS_DHE_RSA_WITH_AES_128_CBC_SHA enabled
TLS_DHE_RSA_WITH_AES_256_CBC_SHA enabled
TLS_RSA_WITH_AES_128_CBC_SHA enabled
TLS_RSA_WITH_AES_256_CBC_SHA enabled
\end{verbatim}

The commands listed below display the default settings of SSL/TLS protocols in normal mode:

\begin{verbatim}
Infoblox > show ssl_tls_protocols
TLSv1.0  TLSv1.1  TLSv1.2
Infoblox > show ssl_tls_ciphers
\end{verbatim}
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 enabled
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 enabled
TLS_DHE_RSA_WITH_AES_128_CBC_SHA enabled
TLS_DHE_RSA_WITH_AES_256_CBC_SHA enabled
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 enabled
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 enabled
TLS_RSA_WITH_AES_128_GCM_SHA256 enabled
TLS_RSA_WITH_AES_128_CBC_SHA enabled
TLS_RSA_WITH_AES_256_CBC_SHA enabled
TLS_RSA_WITH_3DES_EDE_CBC_SHA enabled
TLS_RSA_WITH_AES_256_GCM_SHA384 enabled
TLS_RSA_WITH_AES_256_CBC_SHA enabled
TLS_RSA_WITH_AES_256_CBC_SHA256 enabled
TLS_DHE_DSS_WITH_AES_256_CBC_SHA disabled
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA disabled
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA disabled
TLS_DHE_DSS_WITH_AES_128_CBC_SHA disabled
TLS_RSA_WITH_RC4_128_SHA disabled
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 disabled
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 disabled
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 disabled
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 disabled

Audit Log

The audit log contains a record of all TOE administrative activities. The stored audit records in the audit trail are protected from unauthorized modifications and deletion. For more information about the audit log, see Using the Audit Log. Note that the detailed and brief log types do not depend on the CC mode.

Following are the events that are logged and examples of their corresponding audit log messages:

Identification and Authentication

Event: Enable FIPS mode.
Message: 2011-10-19 19:48:37.299Z [admin]: Login_Allowed - - to=Serial/040Console apparently_via=Direct auth=Local group=.admin-group

Event: Disable FIPS mode.
Message: 2011-10-19 19:48:37.299Z [admin]: Login_Allowed - - to=Serial/040Console apparently_via=Direct auth=Local group=.admin-group

Event: Invalid password when logging in to the WebUI.
Message: 2011-10-19 14:02:32.750Z [admin]: Login_Denied - - to=Serial/040Console apparently_via=Direct error=invalid_login_or_password

Event: Number of attempts exceeds the limit when logging in to the WebUI.
Invalid password when logging in to the CLI.

**Event:** 2011-10-19 14:02:32.750Z [admin]: Login_Denied - - to=Serial\040Console apparently_via=Directerror=invalid\040login\040or\040password

Number of attempts exceeds the limit when logging in to the CLI.

**Event:** 2011-10-19 14:05:23.217Z [admin]: Login_Denied - - to=Serial\040Console apparently_via=Directerror=failed\040logins\040exceed\040limit

Enable Common Criteria mode

**Event:** 2011-10-19 19:48:37.299Z [admin]: Login_Allowed - - to=Serial\040Console apparently_via=Directauth=Local group=.admin-group

**Message:** 2011-10-19 19:48:48.705Z [admin]: Called - set_cc_mode: Args cc_mode_enabled="true"

Disable Common Criteria mode:

**Event:** 2011-10-19 19:48:37.299Z [admin]: Login_Allowed - - to=Serial\040Console apparently_via=Directauth=Local group=.admin-group

**Message:** 2011-10-19 19:48:48.705Z [admin]: Called - set_cc_mode: Args cc_mode_enabled="false"

Login successful

**Event:** 2011-10-19 19:48:48.706Z [USER\040admin]: rebooted the system

**Message:** 2011-10-19 12:43:47.375Z [user]: First_Login - - to=AdminConnector ip=127.0.0.1 auth=LOCALgroup=admin-group apparently_via=GUI first login

**Message:** 2011-10-19 12:44:45.962Z [user]: Password_Reset - - to=AdminConnector auth=LOCALgroup=admin-group apparently_via=GUI

**Message:** 2011-10-19 13:17:29.257Z [user]: Password_Expired - - to=AdminConnector ip=127.0.0.1 auth=LOCALgroup=admin-group apparently_via=GUI

**Message:** 2011-10-19 13:07:33.343Z [user]: Password_Reset_Error - - to=AdminConnector auth=LOCALgroup=admin-group apparently_via=GUI

**Quotas**

**Event:** Upload file limit reached.
**Message:** user manojk-vm httpd[]: err User {0} tried to upload the file. File {1} with size 272629904 kBytes is greater than maximum size allowed. Maximum size is 102400 kBytes.

**LDAP**

**Event:** Establishment of session
**Message:** 2011-10-27T07:50:59-04:00 user epbyminw0065t2 python[]: notice Connection established:success

**Event:** Failure to establish a session
**Message:** 2011-10-27T07:50:38-04:00 user epbyminw0065t2 python[]: err 10.6.11.249: AD user authentication timed out

**Message:** 2011-10-27T07:51:02-04:00 user epbyminw0065t2 python[]: err Connection timed out

**Message:** 2011-10-27T07:51:00-04:00 user epbyminw0065t2 python[]: err SSL handshake failed.
**Message:** 2011-10-27T07:51:02-04:00 user epbyminw0065t2 python[]: err SSL handshake failed. Cannot verify server certificate.

**GSS-TSIG**

**Event:** Invalid size specified for algorithm HMAC-SHA256
**Message:** 2011-10-19T17:57:12-04:00 user EPBYMINW2856 httpd[]: err TSIG key generation failure: Size 512 can not be used with algorithm HMAC-SHA256
Event: Invalid algorithm specified in Common Criteria mode
Message: 2011-10-19T18:12:22-04:00: user EPBYMINW2856 httpd[78497]: err TSIG key (keylen = 256, alginame = HMAC-MD5) generation error: Only HMAC-SHA256 available in CC mode.

Event: Algorithm restriction
Message: Only AES128_CTS_HMAC_SHA1_96 or AES256_CTS_HMAC_SHA1_96 algorithms are allowed in CC mode. Current algorithm is DES_CBC_CRC.

TSIG CSV Import/Export

Event: Import error (TSIG algorithm is not allowed in Common Criteria mode)
Message: 2011/10/20 09:38:42.496 [24473 /usr/bin/python]/infoblox/common/lib/python/infoblox/one/csv_import_function.py:601
write_to_error_file(): Import Error:authzone.zone.com,FORWARD,,,,,,,False,False,False,,1.2.3.4/1.2.3.4/False/False/True/ext_sec_key/ut29ROLaJwty6a%2Fhsgg0wA==,infoblox.localdomain,False,,,,,,,,,,,,,2,,default,Authoritative-Line 2: Insertion aborted due to IBDataError?: IB.Data:TSIG algorithm used for TSIG key name 'ext_sec_key' is not allowed in CC mode.

"set" commands

Message: 2011-10-19 13:14:04.030Z [admin]: Called - set_snmptrap: Args variable="sysName.0", address="10.120.20.31"
Message: 2011-10-19 13:25:31.704Z [admin]: Called - set_security: Args address="10.120.20.31",netmask="255.255.255.0"
Message: 2011-10-19 13:38:42.989Z [admin]: Called - set_network: Args ip_address="10.120.20.34 from 10.120.20.31",netmask="255.255.255.0 from 255.255.255.0",gateway_address="10.120.20.1 from 10.120.20.1"
Message: 2011-10-19 09:53:53.595Z [admin]: Called - set_inet_address: Args address="10.120.20.34 from 10.120.20.31",netmask="255.255.255.0 from 255.255.255.0",gateway_address="10.120.20.1 from 10.120.20.1"
Message: 2011-10-19 14:19:25.282Z [admin]: Called - set_host_consistency_check: Args host_consistency_check=on from off
Message: 2011-10-19 14:30:54.628Z [admin]: Called - set_named_recv_sock_buf_size: Args udp_so_rcvbuf="122 from (null)"

CLI Top Level Commands

Message: 2011-10-19 11:00:17.917Z [admin]: Called - delete_backup: Args filename="BACKUP_6.bkp"
CLI Emergency Commands

<table>
<thead>
<tr>
<th>Message</th>
<th>Time</th>
<th>User</th>
<th>Command</th>
<th>Args</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-10-19 12:58:11.738Z</td>
<td>[USER/040admin]</td>
<td>rotated the previous audit log to audit.log.0.gz</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Syslog

NIOS appliances generate syslog messages that you can view through the Syslog viewer and download to a directory on your management station. For more information about syslog, see Using a Syslog Server.

Following are the events that are logged and examples of their corresponding syslog messages:

Establishment/Termination of an HTTPS Session

<table>
<thead>
<tr>
<th>Event</th>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event: Generation of RSA key failed.</td>
<td>Oct 19 09:15:01</td>
<td>EPBYMINW006ST1 httpd[2115]</td>
<td>cryptographic key generation failed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event: Session is terminated.</td>
<td>Oct 19 09:15:01</td>
<td>EPBYMINW006ST1 httpd[2115]</td>
<td>Session terminated (remote address: 10.6.11.249)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event: Session is established.</td>
<td>Oct 19 08:54:42</td>
<td>EPBYMINW006ST1 httpd[2314]</td>
<td>Session has been established (remote address: 10.6.11.249)</td>
</tr>
</tbody>
</table>

Establishment/Termination of a TLS Session

<table>
<thead>
<tr>
<th>Event</th>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event: Session has been established.</td>
<td>Oct 19 08:38:08</td>
<td>EPBYMINW006ST1 openvpn[1552]</td>
<td>Session has been established (remote address: 10.6.11.249)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event: Signing failure (constructed message, it is not trivial to obtain it into the syslog).</td>
<td>Oct 19 08:45:01</td>
<td>EPBYMINW006ST1 openvpn[1582]</td>
<td>cryptographic operation failed: signature</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Time</th>
<th>User</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event: Session was not established.</td>
<td>Oct 19 08:50:21</td>
<td>EPBYMINW006ST1 openvpn[1701]</td>
<td>Failed to establish a session (remote address: 10.6.11.249), error 1115 (SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed)</td>
</tr>
</tbody>
</table>
Event: Packet was not verified.
Message: "Oct 19 08:55:25 EPBYMINW0065T1 openvpn[1815]: Packet verification fails (remote address: 10.6.11.249)"

Random Number Generation Process
[2011/10/19 10:13:46.282] (26360 /infoblox/one/bin/ib_prngd_control) : ib_prngd daemon is not running while CC mode is enabled
[2011/10/19 10:13:46.324] (26368 /infoblox/one/bin/ib_prngd) main.c:202 main(): ib_prngd daemon starting up...
[2011/10/19 10:13:46.700] (26368 /infoblox/one/bin/ib_prngd) main.c:214 main(): Setting FIPS mode OK
[2011/10/19 10:13:46.400] (26368 /infoblox/one/bin/ib_prngd) main.c:214 main(): Setting FIPS mode FAILED
Note: For more information about FIPS, see Appendix D: Guidance Document Supplement for Federal Information Processing Standard.
[2011/10/19 10:13:46.700] (26368 /infoblox/one/bin/ib_prngd) main.c:125 rename_rnd_dev(): Moving /dev/random to /dev/random_backup OK
[2011/10/19 10:13:46.700] (26368 /infoblox/one/bin/ib_prngd) main.c:127 rename_rnd_dev(): Moving /dev/urandom to /dev/urandom_backup OK
[2011/10/19 10:13:46.700] (26368 /infoblox/one/bin/ib_prngd) main.c:234 main(): Creating FIFO /dev/ib_random OK
[2011/10/19 10:13:46.700] (26368 /infoblox/one/bin/ib_prngd) main.c:158 symlink_rnd_dev(): Symlinking /dev/random to /dev/ib_random OK
[2011/10/19 10:13:46.700] (26368 /infoblox/one/bin/ib_prngd) main.c:160 symlink_rnd_dev(): Symlinking /dev/urandom to /dev/ib_random OK
[ TIME NOT KNOWN ] (26368) main.c:signal_handler{}: ib_prngd received SIGTERM signal....exiting.
[ TIME NOT KNOWN ] (26368) main.c:signal_handler{}: ib_prngd received SIGINT signal....exiting.
[ TIME NOT KNOWN ] (26368) main.c:signal_handler{}: ib_prngd received SIGQUIT signal....exiting. 
[2011/10/19 10:13:49.205] (26368 /infoblox/one/bin/ib_prngd) main.c:135 rename_rnd_dev(): Renaming /dev/random back OK
[2011/10/19 10:13:49.205] (26368 /infoblox/one/bin/ib_prngd) main.c:141 rename_rnd_dev(): Renaming /dev/urandom back OK
[2011/10/19 10:13:49.205] (26368 /infoblox/one/bin/ib_prngd) main.c:255 main(): Removing custom FIFO /dev/ib_random OK
[2011/10/19 10:13:49.205] (26368 /infoblox/one/bin/ib_prngd) main.c:255 main(): Removing custom FIFO /dev/ib_random FAILED
[2011/10/19 10:13:49.205] (26368 /infoblox/one/bin/ib_prngd) main.c:141 rename_rnd_dev(): Renaming /dev/urandom back FAILED
[2011/10/19 10:13:49.205] (26368 /infoblox/one/bin/ib_prngd) main.c:255 main(): Removing custom FIFO /dev/ib_random FAILED
[2011/10/19 10:13:49.205] (26368 /infoblox/one/bin/ib_prngd) main.c:135 rename_rnd_dev(): Renaming /dev/random back FAILED
[2011/10/19 10:25:22.931] (26557 /infoblox/one/bin/ib_prngd) main.c:189 main(): Error! /infoblox/one/bin/ib_prngd is already running
[2011/10/19 10:26:58.107] (26560 /infoblox/one/bin/ib_prngd) main.c:52 self_test(): OpenSSL FIPS mode functionality self test OK
[2011/10/19 10:26:58.107] (26560 /infoblox/one/bin/ib_prngd) main.c:52 self_test(): OpenSSL FIPS mode functionality self test FAILED
Note: For more information about FIPS, see Appendix D: Guidance Document Supplement for Federal Information Processing Standard.

Failures on Invoking Functionality
Event: Invalid size specified for algorithm HMAC-SHA256.
Message: 2011-10-19T17:57:12-04:00 user EPBYMINW2856 httpd[]: err TSIG key generation failure: Size 512 can not be used with algorithm HMAC-SHA256

Event: Invalid algorithm specified in Common Criteria mode.
Message: 2011-10-19T18:22:04-04:00 user EPBYMINW2856 httpd[]: err TSIG key (keylen = 256, algname = HMAC-MD5) generation error : Only HMAC-SHA256 available in CC mode.

Open VPN
Event: Generation of RSA key failed
Message: Oct 19 08:38:08 EPBYMINW0065T1? openvpn[1415]: cryptographic key generation failed

Event: Session has been established
Message: Oct 19 08:38:08 EPBYMINW0065T1? openvpn[1552]: Session has been established (remote address: 10.6.11.249)

Event: HMAC failure
Message: Oct 19 08:41:01 EPBYMINW0065T1? openvpn[1567]: cryptographic key generation failed: HMAC

Event: Signing failure
Message: Oct 19 08:45:01 EPBYMINW0065T1? openvpn[1582]: cryptographic operation failed: signature

Event: Encryption failure

Event: Session was not established
Message: Oct 19 08:50:21 EPBYMINW0065T1? openvpn[1701]: Failed to establish a session (remote address: 10.6.11.249), error 1115 (SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed)

Event: Packet was not verified
Message: Oct 19 08:55:25 EPBYMINW0065T1? openvpn[1815]: Packet verification fails (remote address: 10.6.11.249)

HTTPS
Event: Generation of RSA key failed
Message: Oct 19 09:15:01 EPBYMINW0065T1? httpd[2115]: cryptographic key generation failed

Event: Session is terminated
Message: Oct 19 09:15:01 EPBYMINW0065T1? httpd[2115]: Session terminated (remote address: 10.6.11.249)

Event: Failed to establish a session
Message: Oct 19 08:50:21 EPBYMINW0065T1? httpd[2115]: Failed to establish a session (remote address: 10.6.11.249), error 1115 (SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed)

Event: Session is established
Message: Oct 19 08:54:42 EPBYMINW0065T1? httpd[2314]: Session has been established (remote address: 10.6.11.249)

Message: Failed to establish a session (remote address: 10.6.11.249), error 1115 (SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed)

Event: HMAC failure

DNS
Message: 2011-10-18T13:37:33+00:00 daemon (none) named[4456]: err client 10.32.2.108#47160: request has invalid signature: TSIG sha256cc: tsig verify failure (BADKEY) 2011-10-18T13:37:33+00:00 daemon (none) named[4456]: err client 10.32.2.108#47160: request has invalid signature: TSIG sha256cc: tsig verify failure (BADKEY)

DHCP
Message: 2011-10-26T12:33:30-04:00 user EPBYMINW2994t1 infoblox_crypt[]: err cryptographic operation failed: decryption
Message: 2011-10-26T12:34:33-04:00 user EPBYMINW2994t1 infoblox_crypt[]: err cryptographic operation failed: encryption
Message: 2011-10-26T12:35:53-04:00 user EPBYMINW2994t1 infoblox_crypt[]: err cryptographic operation failed: RSA verify signature
Message: 2011-10-26T12:38:56-04:00 user EPBYMINW2994t1 infoblox_crypt[]: err cryptographic operation failed: RSA signing

Quotas
Event: When the administration backend is overloaded by too much combined GUI and API traffic, a message like this is logged to syslog (it is not associated with any user).
Message: 2011-10-31T23:42:21+00:00 daemon (none) httpd[]: warning Too many administration connections Event: Disk space limit was changed and is below the disk usage.
Message: 2011-10-02T00:24:54+00:00 user manojk-vm httpd[]: err Storage Limit has been lowered and usage now exceeds the limit, Usage: 150 MB, Limit :100 MB

Event: Disk space limit reached.
Message: 2011-10-02T00:24:54+00:00 user manojk-vm httpd[]: err Exceed the TFTP Storage limit, User name:user1, Used Storage:2048 B, File name :a.zip, File size :272629904 B, Limit :102400 B

Open SSL
Event: FIPS self test failed.
Note: For more information about FIPS, see Appendix D: Guidance Document Supplement for Federal Information Processing Standard.
Message: 140576691959464:error:140A9129:SSL routines:SSL_CTX_new:only tls allowed in fips mode:ssl_lib.c:1527:
Message: 139852903503528:error:0A07C06E:digital envelope routines:EVP_DigestInit_ex:unknown cipher:digest.c:248:

Event: Error setting digest MD5.
Message: 140418599392936:error:141D00B9:SSL routines:SSL_CTX_set_cipher_list:no cipher match:ssl_lib.c:1282:

Replay Detection
Event: OpenVPN

Event: HTTPS
= 123456789

GSS-TSIG
Appendix D Guidance Documentation Supplement for Federal Information Processing Standard

The FIPS (Federal Information Processing Standard) 140-2 is a computer security standard that defines a set of rules and regulations to validate cryptographic modules. It gives assurance that the product satisfies a set of internationally recognized security standards.

This document provides additional guidance on the secure installation of the Target of Evaluation (TOE) for FIPS. The TOE includes the following Infoblox appliances that are network appliances and provides delivery of IP network services and management, Grid and HA configuration:

- Virtual appliances (certificate number 3330),
- Trinzic physical appliances: TE-825, TE-1425, TE-2225, TE-4015,
- TE-4025 DDI appliances (certificate number 3332).

Note that the module must run NIOS version 8.2.6 with Hotfix-NIOS_8.2.6-371069_J67303_FIPS_2-6f0806b9bc9cbdcb9837391bb5a86a26-Tue-Aug-21-22-24-14-2018. For more information about the FIPS mode, refer to the following:

https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program
The Trinzic appliances can be made compliant with Common Criteria and FIPS 140-2 security standards. They contain a FIPS and Common Criteria certified cryptographic module that is utilized in both FIPS and/or Common Criteria modes. To comply with FIPS 140-2 requirements, you must properly affix the security label on the appliance. For more information, refer to the respective Installation Guide. To enable Common Criteria mode, execute the commands mentioned in Enabling/Disabling Common Criteria Mode. When you enable the Common Criteria mode, only the respective mode is enabled in the device.

Infoblox recommends that you configure FIPS mode if you want to configure only FIPS or both Common Criteria and FIPS certifications as it covers FIPS specific functionality (additional required POST testing) as well as Common Criteria certified cryptographic module and audit records. FIPS includes all features of Common Criteria mode and setting FIPS mode implicitly sets the Common Criteria mode. When you enable the FIPS mode in your device, it enables both FIPS and Common Criteria mode. This appendix is a supplement to Appendix C in which all information also applies to FIPS. For more information, see Guidance Documentation Supplement for Common Criteria. To enable and disable FIPS, see Enabling/Disabling FIPS.

To ensure that your appliance is FIPS compliant, make sure that your hardware and software settings match the evaluated configuration that was certified for FIPS. This document provides clarifications and changes to the Infoblox Administrator Guide and Infoblox CLI Guide, and should be used as the guiding document for installation of the TOE in the FIPS evaluated configuration.

This appendix contains the following sections:

- Managing Administrators
- Authenticating Admins using Remote Authentication
- Enabling/Disabling FIPS
- Installing FIPS Label on an Infoblox Trinzic Appliance
- FIPS (Federal Information Processing Standard) Certification
- List of NIOS Algorithms

Secure Initialization

Follow the instructions mentioned below to initialize the module in to FIPS approved mode of operation. Failure to follow the instructions below may result in a non-compliant system:

- The module must be running NIOS version 8.2.6 with Hotfix-NIOS_8.2.6-371069_J67303_FIPS_2-6f0806b9bc9837391bb5a86a26-Tue-Aug-21-22-24-14-2018.
- Apply tamper evident labels to the appliance as mentioned in the respective installation guide.
- Enable FIPS mode using the set fips_mode command. For more information, see Enabling/Disabling FIPS.
- The Minimum Password Length must be at least 6 characters. For more information, see Setting Password Restrictions for Local Admins.
- You cannot use the keys/CSPs (Cryptographic Critical Security Parameters), which are generated in a FIPS mode, in a non-FIPS mode and vice-versa.
- Infoblox does not support certain services while operating in the FIPS approved mode.

Non-Approved Services

Enabling any of the listed services may result in a non-compliant system.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Access</td>
<td>Support Access SSH service</td>
</tr>
<tr>
<td>BloxTools</td>
<td>Pre-installed environment to host custom web-based applications</td>
</tr>
<tr>
<td>RADIUS authentication</td>
<td>Remote user authentication using RADIUS protocol</td>
</tr>
<tr>
<td>TACACS+ authentication</td>
<td>Remote user authentication using TACACS+ protocol</td>
</tr>
<tr>
<td>Cisco ISE Integration</td>
<td>Managing Cisco ISE Integration</td>
</tr>
<tr>
<td>Microsoft Server</td>
<td>Managing Microsoft DNS/DHCP servers using BIND</td>
</tr>
<tr>
<td>SNMPv1/v2</td>
<td>Simple Network Management Protocol versions 1 and 2. This is valid for both Network Insight Discovery services as well as the NIOS SNMP.</td>
</tr>
</tbody>
</table>
Managing Administrators

A user must have an admin account to log in to the TOE. Each admin account belongs to an admin group, which contains roles and permissions that determine the tasks a user can perform.

The TOE provides a default superuser admin group, called admin-group, with one superuser administrator, admin. The default superuser admin can log in to the TOE, using the default user name admin and password infoblox. Superuser admins are the security admins and have full access and control of all the operations of a TOE. Note that you must change the default user name and password of the default superuser admin to prevent unauthorized access to the TOE. For more information about the tasks that superusers and limited-access admins can perform, see Guidance Documentation Supplement for Common Criteria.

Setting Password Restrictions for Local Admins

All admins are required to enter a username and password when they log in to Grid Manager or the CLI. A superuser can set minimum password length through Grid Manager. To set minimum password length, from the Grid tab -> Grid Properties -> Edit. In the Grid Properties editor, select the Password tab and specify the minimum number of characters that are required in a password. Note that the minimum password length must be between 4 and 64 characters. Ensure that the Minimum Password Length is at least 6 characters. You can specify character types, such as lowercase or uppercase characters, that are allowed in the password and the number of required character changes from the previous password, whether passwords expire and their duration. For information about defining the password policy, see Managing Passwords. TOE locks the user after five consecutive failed logins from the same IP address within a minute.

Authenticating Admins using Remote Authentication

NIOS supports the following remote authentication methods: AD domain controllers, RADIUS, LDAP, TACACS+, and Two-factor authentication and authenticates admins whose credentials are stored remotely on these servers. For more information, see About Remote Admins.

AD domain controllers

The minimum timeout value for AD domain controllers is one second. You must add domain controllers to an AD authentication server group and specify the minimum timeout value from the Grid Manager. To add domain controllers, from the Administration tab -> Authentication Server Groups tab -> Active Directory Services subtab, click the Add icon and enter the details in the Add Active Directory Authentication Service wizard. You can specify either SSL or CA Certificates as the encryption method. If you enable SSL encryption for AD, then CA certificates are used for LDAP communication. For more information, see Authenticating Admins Using Active Directory.

RADIUS

In this remote authentication process, NIOS sends an authentication request to a RADIUS server group. This is controlled by CC/FIPS mode. To configure a RADIUS authentication server group, from the Administration tab -> Authentication Server Groups tab, click the Add icon in the RADIUS Services subtab, and specify the details in the Add RADIUS Authentication Service wizard. For more information, see Authenticating Admins Using RADIUS.

Note: Do not use the RADIUS authentication method when you operate in the FIPS mode.

LDAP

NIOS authenticates admin accounts by verifying user names and passwords against LDAP. If you select SSL as the encryption type for LDAP, then the prefix of the LDAP URL is set to ldaps. Otherwise, it is set to ldap. To set encryption type for an LDAP server group, from the Administration tab -> Authentication Server Groups tab, click the Add icon in the LDAP Services subtab, and specify the details in the Add LDAP Authentication Service wizard. When you enable the common criteria mode, LDAP sets minimal TLS protocol to TLS 1.0 and TLS cipher suites to the following: "-ALL:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:AES256-SHA:AES128-SHA:". For more information, see Authenticating Admins Using LDAP.

TACACS+

TACACS+ provides separate authentication, authorization, and accounting services. This is controlled by CC/FIPS mode. You can configure a custom service, infoblox, on the TACACS+ server, and then define a user group and specify the group name in the custom attribute infoblox-admin-group. To configure a TACACS+ authentication server group, from the Administration tab -> Authentication Server Groups tab, click the Add icon in the TACACS+ Services subtab, and specify the details in the Add TACACS+ Service wizard. For more information, see Authenticating Admin Accounts Using TACACS+.

Note: Do not use the TACACS+ authentication method when you operate in the FIPS mode.
Two-factor authentication

You can configure NIOS to use the two-factor authentication method to authenticate users based on X.509 client certificates. In this authentication method, NIOS first negotiates SSL/TLS client authentication to validate client certificates and then authenticates the admins based on the configured authentication policy. You must first configure an authentication policy, and then configure and enable the certificate authentication service for the two-factor authentication to take effect. To configure and enable the two-factor authentication service, from the Administration tab -> Authentication Server Groups tab, click the Add icon in the Certificate Authentication Services subtab. OCSP service validates the certificates.

NIOS performs lookup against local users by default. You can enable remote lookup for user membership by choosing an Active Directory as authentication service and specifying the username and password for this service. Note that the password must not be empty. For more information, see Authenticating Admins Using Two-Factor Authentication.

Enabling/Disabling FIPS

You can enable and disable FIPS mode from the Infoblox CLI only. Do the following to set FIPS mode on the appliance:

1. Log in to the Infoblox CLI using a superuser account.
2. Enable FIPS mode using the following command:
   `Infoblox > set fips_mode`
3. Reboot the appliance, connect to the serial console and use the following command to check if the FIPS mode is enabled:
   `Infoblox > show fips_mode`
4. Verify if the following files exist in the directories mentioned:
   - `/infoblox/security/keys/integrity.key`
   - `/infoblox/security/keys/integrity.pem`
   - `/infoblox/security/sha256sum_bin.txt`
   - `/infoblox/security/sha256sum_bin.txt.sha256`

   **Note:** You cannot enable the Common Criteria mode when the FIPS mode is enabled, but note that Common Criteria mode is a subset of the FIPS mode. When you enable FIPS mode in your device, it enables both FIPS and Common Criteria mode. For more information about the Common Criteria mode, see Appendix C Guidance Documentation Supplement for Common Criteria.

For more information about the commands mentioned above, refer to the Infoblox CLI Guide. Upgrade the TOE only when the FIPS mode is enabled. The security administrator will be able to upgrade to a validated release package only. The security administrator can verify the TOE by the version number included in the file name as well as through the administrative interface before and after the upgrade. Refer to the Release Notes of the NIOS version to which the TOE is upgrading for additional upgrade instructions. To upgrade the TOE through Grid Manager, see Upgrading NIOS Software.

To revert the TOE to the previously running software, ensure that the FIPS mode is enabled. For more information, see Reverting the Grid to the Previously Running Software.

To disable FIPS mode, execute the following command: `Infoblox > set fips_mode`. You can verify if the FIPS mode is disabled using the following command: `Infoblox > show fips_mode`. Ensure that the files `/infoblox/security/sha256sum_bin.txt` and `/infoblox/security/sha256sum_bin.txt.sha256` are deleted.

To clear FIPS mode on an appliance, log in to the Infoblox CLI and execute the command: `reset all`.

The TOE reboots and goes through boot time self tests. If the test fails, the TOE goes into a loop and displays an error message on the serial console and the LCD. Otherwise, it displays the Login prompt after the self tests. Multi-Grid management is enabled as soon as Grid support becomes FIPS capable.

Note the following:

- When you configure a Grid Master and enable a certain, either CC or FIPS, mode in the Grid Master and then configure a Grid member with a different mode than that of the Grid Master, the member automatically takes the same mode as the Grid Master when you add this member to the Grid Master. For example, if the Grid Master is in FIPS mode and the Grid member is CC mode enabled, the Grid member becomes FIPS enabled when you add this member to the Grid.
- Consider an HA Grid Master with a certain, either CC or FIPS, mode enabled in the active node. When you join a passive node to the HA Grid Master, it automatically takes the same mode as the Grid Master in the active node. For example, if FIPS is enabled in the active node, then the passive node too becomes FIPS enabled when you join it to the HA Grid Master even though it was in CC mode earlier.
- When the HA pair is enabled, you cannot enable or disable either the CC or FIPS mode on the active or passive nodes.

Infoblox suggests that you do the following for an HA pair:

- Set either CC or FIPS mode on each node before building an HA pair.
- Set both the nodes of an HA pair in the same mode, that is either in the CC mode, or FIPS mode, or none.

Installing FIPS Label on an Infoblox Trinzic Appliance
The module must be opaque within the visible spectrum and have tamper evident labels for doors or removable covers in order to be compliant with FIPS 140-2 Security Level 2 requirements. Infoblox provides tamper evident labels (TEPs) which you must install on the appliance to operate in the FIPS approved mode. The Crypto Officer is responsible for inspecting the TEPs regularly for signs of tamper, and should contact Infoblox customer support if any signs of tamper are found.

Note that the SKU is IB-FIPS and includes 9 labels for each SKU order. The FIPS label is as shown below:

For more information about how to install FIPS label on the following appliances, refer to the respective installation guide: TE-825, TE-1425, TE-225, TE-4015, and TE-4025.

**FIPS (Federal Information Processing Standard) Certification**

You must configure the TOE to perform cryptographic operations using FIPS. To configure the FIPS mode setting, use the set fips_mode command. Enter y to enable and confirm the setting and another y to confirm that you are ready to continue.

Note: Infoblox does not recommend upgrade from a non FIPS system to a FIPS system.

Following are the events that are logged and examples of their corresponding syslog messages:

**GSS-TSIG**

**Event**: ISC library in BIND sources: Definition of element hsha (of type pk11_context_t) in the union ctx in function sign()
**Message**:./fipscc_nios/bind9/lib/isccc/cc.c:242: isc_hmacsha1_t hsha;

**Event**: ISC library in BIND sources: A HMAC-SHA1 case in algorithm switch block in the function sign()
**Message**:./fipscc_nios/bind9/lib/isccc/cc.c:264: case ISCCC_ALG_HMACSHA1:

**Event**: ISC library in BIND sources: a HMAC-SHA1 context initialized
**Message**: ./fipscc_nios/bind9/lib/isccc/cc.c:265: isc_hmacsha1_init(&ctx.hsha, secret->rstart, 

**Event**: ISC library in BIND sources: a HMAC-SHA1 context updated
**Message**: ./fipscc_nios/bind9/lib/isccc/cc.c:267: isc_hmacsha1_update(&ctx.hsha, data, length);

**Event**: ISC library in BIND sources: a HMAC-SHA1 context signed
**Message**: ./fipscc_nios/bind9/lib/isccc/cc.c:268: isc_hmacsha1_sign(&ctx.hsha, digest, 

**Event**: ISC library in BIND sources: macro name
**Message**: ./fipscc_nios/bind9/lib/isccc/cc.c:269: ISC_SHA1_DIGESTLENGTH;

**Event**: ISC library in BIND sources:
**Message**: ./fipscc_nios/bind9/lib/isccc/cc.c:270: source.rend = digest + ISC_SHA1_DIGESTLENGTH; macro name

**Event**: ISC library in BIND sources: definition of element hsha (of type pk11_context_t) in the union ctx in function verify()
**Message**: ./fipscc_nios/bind9/lib/isccc/cc.c:389: isc_hmacsha1_t hsha;

**Event**: ISC library in BIND sources: a HMAC-SHA1 case in algorithm switch block in the function verify()
**Message**: ./fipscc_nios/bind9/lib/isccc/cc.c:428: case ISCCC_ALG_HMACSHA1:

**Event**: ISC library in BIND sources: a HMAC-SHA1 context initialized
**Message**: ./fipscc_nios/bind9/lib/isccc/cc.c:429: isc_hmacsha1_init(&ctx.hsha, secret->rstart,
Event: ISC library in BIND sources: a HMAC-SHA1 context updated
Message: ./fipscc_nios/bind9/lib/isccc/cc.c:431: isc_hmacsha1_update(&ctx.hsha, data, length);

Event: ISC library in BIND sources: a HMAC-SHA1 context signed
Message: ./fipscc_nios/bind9/lib/isccc/cc.c:432: isc_hmacsha1_sign(&ctx.hsha, digest,

Event: ISC library in BIND sources: macro name
Message: ./fipscc_nios/bind9/lib/isccc/cc.c:433: ISC_SHA1_DIGESTLENGTH);

Event: ISC library in BIND sources: macro name
Message: ./fipscc_nios/bind9/lib/isccc/cc.c:434: source.rend = digest + ISC_SHA1_DIGESTLENGTH;

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/bind9/include/isccc/cc.h:48:#define ISCCC_ALG_HMACSHA1 161

Event: BIND sources macro usage
Message: ./fipscc_nios/bind9/lib/bind9/check.c:44:#ifdef HMAC_SHA1_SIT

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/bind9/check.c:45:#include <isc/sha1.h>

Event: BIND sources macro usage
Message: ./fipscc_nios/bind9/lib/bind9/check.c:1195:#ifdef HMAC_SHA1_SIT

Event: BIND sources macro usage
Message: ./fipscc_nios/bind9/lib/bind9/check.c:1197: isc_buffer_usedlength(&b) != ISC_SHA1_DIGESTLENGTH) {

Event: BIND sources string literal
Message: ./fipscc_nios/bind9/lib/bind9/check.c:1199: "SHA1 sit-secret must be on 160 bits");

Event: BIND sources: element of static constant array (definition) of algorithm names

Event: BIND sources macro usage
Message: ./fipscc_nios/bind9/lib/bind9/check.c:2603: if ((alg == DST_ALG_RSASHA1 || alg == DST_ALG_RSAMD5) &&

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:20: * This code implements the HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/hmacsha.c:31:#include

Event: ISC library in BIND: HMAC-SHA1 hash init function isc_hmacsha1_init() which is a wrapper for HMAC_Init()
Message: ./fipscc_nios/bind9/lib/hmacsha.c:44:isc_hmacsha1_init(isc_hmacsha1_t *ctx, const unsigned char *key,
Event: ISC library in BIND: HMAC-SHA1 context gets initialized in function isc_hmacsha1_init() by calling HAMC_Init() using hash function EVP_sha1() as an argument
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:49: (int) len, EVP_sha1()) == 1);

Event: ISC library in BIND: HMAC-SHA1 context gets initialized in function isc_hmacsha1_init() by calling HAMC_Init() using hash function EVP_sha1() as an argument
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:51: HMAC_Init(ctx, (const void *) key, (int) len, EVP_sha1());

Event: ISC library in BIND: definition of the function isc_hmacsha1_invalidate() (which is a wrapper for HMAC_CTX_cleanup()) with an argument of type isc_hmacsha1_t (which is a type defined for pk11_context_t, which in turn is struct pk11_context)
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:56:isc_hmacsha1_invalidate(isc_hmacsha1_t *ctx) {

Event: ISC library in BIND: definition of the function isc_hmacsha1_update() (which is a wrapper for HMAC_Update()) with argument of type isc_hmacsha1_t (which is a type defined for pk11_context_t, which in turn is struct pk11_context)
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:61:isc_hmacsha1_update(isc_hmacsha1_t *ctx, const unsigned char *buf,

Event: ISC library in BIND: definition of the function isc_hmacsha1_sign() (which is an extension for HMAC_Final())
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:72:isc_hmacsha1_sign(isc_hmacsha1_t *ctx, unsigned char *digest, size_t len) {

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:73: unsigned char newdigest[ISC_SHA1_DIGESTLENGTH];

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:75: REQUIRE(len <= ISC_SHA1_DIGESTLENGTH);

Event: ISC library in BIND: HMAC-SHA1 hash init function isc_hmacsha1_init() with an argument *ctx of type isc_hmacsha1_t (which is a type defined for pk11_context_t, which in turn is struct pk11_context)
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:269:isc_hmacsha1_init(isc_hmacsha1_t *ctx, const unsigned char *key,

Event: ISC library in BIND: HMAC-SHA1 hash invalidate function isc_hmacsha1_invalidate() with an argument *ctx of type isc_hmacsha1_t (which is a type defined for pk11_context_t, which in turn is struct pk11_context)
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:298:isc_hmacsha1_invalidate(isc_hmacsha1_t *ctx) {

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:299: CK_BYTE garbage[ISC_SHA1_DIGESTLENGTH];

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:300: CK_UULONG len = ISC_SHA1_DIGESTLENGTH;

Event: ISC library in BIND: HMAC-SHA1 hash update function isc_hmacsha1_update() with an argument *ctx of type isc_hmacsha1_t (which is a type defined for pk11_context_t, which in turn is struct pk11_context)
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:313:isc_hmacsha1_update(isc_hmacsha1_t *ctx, const unsigned char *buf,

Event: ISC library in BIND: HMAC-SHA1 hash sign function isc_hmacsha1_sign() with an argument *ctx of type isc_hmacsha1_t (which is a type defined for pk11_context_t, which in turn is struct pk11_context)
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:325:isc_hmacsha1_sign(isc_hmacsha1_t *ctx, unsigned char *digest, size_t len) {

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:327: CK_BYTE newdigest[ISC_SHA1_DIGESTLENGTH];
Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:328: CK ULONG psl = ISC_SHA1_DIGESTLENGTH;

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:330: REQUIRE(len <= ISC_SHA1_DIGESTLENGTH);

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:639: * Start HMAC-SHA1 process. Initialize an sha1 context and digest the key.

Event: ISC library in BIND: HMAC-SHA1 hash init function isc_hmacsha1_invalidate() with an argument *ctx of type isc_hmacsha1_t (which is a type defined for pk11_context_t, which in turn is struct pk11_context)
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:642:isc_hmacsha1_init(isc_hmacsha1_t *ctx, const unsigned char *key,

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:645: unsigned char ipad[ISC_SHA1_BLOCK_LENGTH];

Event: ISC library in BIND: declared variable sha1ctx of type isc_sha1_t (which is defined for type EVP_MD_CTX) for usage within the function isc_hmacsha1_init
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:650: isc_sha1_t sha1ctx;

Event: ISC library in BIND: in the function isc_hmacsha1_init(): calling the function isc_sha1_init() of the same library with an argument named sha1ctx
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:651: isc_sha1_init(&sha1ctx);

Event: ISC library in BIND: in the function isc_hmacsha1_init(): calling the function isc_sha1_update() of the same library with an argument named sha1ctx
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:652: isc_sha1_update(&sha1ctx, key, len);

Event: ISC library in BIND: in the function isc_hmacsha1_init(): calling the function isc_sha1_final() of the same library with an argument named sha1ctx
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:653: isc_sha1_final(&sha1ctx, ctxkey);

Event: ISC library in BIND: from the function isc_hmacsha1_init(): calling the function isc_sha1_init() to initialize the HMAC-SHA1 context
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:657: isc_sha1_init(&ctx->sha1ctx);

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:659: for (i = 0; i < ISC_SHA1_BLOCK_LENGTH; i++)

Event: ISC library in BIND: update the HMAC-SHA1 context by calling the function isc_sha1_update() (it will descend in call of EVP_DigestUpdate())
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:661: isc_sha1_update(&ctx->sha1ctx, ipad, sizeof(ipad));

Event: ISC library in BIND: definition of function isc_hmacsha1_invalidate() which has an argument of type isc_hmacsha1_t (which is struct pk11context in the end)
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:665:isc_hmacsha1_invalidate(isc_hmacsha1_t *ctx) {

Event: ISC library in BIND: from the function isc_hmacsha1_invalidate(): calling isc_sha1_invalidate() with an argument that has "sha1" in its name
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:666: isc_sha1_invalidate(&ctx->sha1ctx);
Event: ISC library in BIND: definition of the function isc_hmacsha1_update() which is a wrapper for isc_sha1_update() and updates the HMAC-SHA1 context by another buffer of bytes
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:675:isc_hmacsha1_update(isc_hmacsha1_t *ctx, const unsigned char *buf,

Event: ISC library in BIND: from the function isc_hmacsha1_sign(): call isc_sha1_update() to update the HMAC-SHA1 context by another buffer of bytes
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:678: isc_sha1_update(&ctx->sha1ctx, buf, len);

Event: ISC library in BIND: macro usage

Event: ISC library in BIND: definition of the function isc_hmacsha1_sign() which computes the signature by finalizing SHA1 operation
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:685:isc_hmacsha1_sign(isc_hmacsha1_t *ctx, unsigned char *digest, size_t len) {

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:686: unsigned char opad[ISC_SHA1_BLOCK_LENGTH];

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:687: unsigned char newdigest[ISC_SHA1_DIGESTLENGTH];

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:690: REQUIRE(len <= ISC_SHA1_DIGESTLENGTH);

Event: ISC library in BIND: from the function isc_hmacsha1_sign(): call isc_sha1_final() to compute the signature by finalizing SHA1 operation
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:691: isc_sha1_final(&ctx->sha1ctx, newdigest);

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:694: for (i = 0; i < ISC_SHA1_BLOCK_LENGTH; i++)

Event: ISC library in BIND: from the function isc_hmacsha1_sign(): call isc_sha1_init() to initialize HMAC-SHA1 context
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:697: isc_sha1_init(&ctx->sha1ctx);

Event: ISC library in BIND: from the function isc_hmacsha1_sign(): call isc_sha1_update() to update HMAC-SHA1 context with new bytes
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:698: isc_sha1_update(&ctx->sha1ctx, opad, sizeof(opad));

Event: ISC library in BIND: from the function isc_hmacsha1_sign(): call isc_sha1_update() to update HMAC-SHA1 context with new bytes
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:699: isc_sha1_update(&ctx->sha1ctx, newdigest, ISC_SHA1_DIGESTLENGTH);

Event: ISC library in BIND: from the function isc_hmacsha1_sign(): call isc_sha1_init() to finalize HMAC-SHA1 context
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:700: isc_sha1_final(&ctx->sha1ctx, newdigest);

Event: ISC library in BIND: from the function isc_hmacsha1_sign(): call isc_sha1_invalidate() to invalidate HMAC-SHA1 context (i.e. call HMAC_CTX_cleanup() underneath)
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:701: isc_hmacsha1_invalidate(ctx);

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:972: * Verify signature - finalize SHA1 operation and reapply SHA1, then

Event: ISC library in BIND: definition of the function isc_hmacsha1_verify() which verifies signatures
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:976:isc_hmacsha1_verify(isc_hmacsha1_t *ctx, unsigned char *digest, size_t len) {

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:977: unsigned char newdigest[ISC_SHA1_DIGESTLENGTH];

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:979: REQUIRE(len <= ISC_SHA1_DIGESTLENGTH);

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/hmacsha.c:980: isc_hmacsha1_sign(ctx, newdigest, ISC_SHA1_DIGESTLENGTH);

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/isc/entropy.c:44:#include <isc/sha1.h>

Event: ISC library in BIND sources: declaration of a variable of type isc_sha1_t (i.e. EVP_MD_CTX)
Message: ./fipscc_nios/bind9/lib/isc/entropy.c:537: isc_sha1_t hash;

Event: ISC library in BIND sources: macro name
Message: ./fipscc_nios/bind9/lib/isc/entropy.c:538: unsigned char digest[ISC_SHA1_DIGESTLENGTH];

Event: ISC library in BIND sources: a HMAC-SHA1 context initialized in function isc_entropy_getdata()
Message: ./fipscc_nios/bind9/lib/isc/entropy.c:612: isc_sha1_init(&hash);

Event: ISC library in BIND sources: a HMAC-SHA1 context updated in function isc_entropy_getdata()
Message: ./fipscc_nios/bind9/lib/isc/entropy.c:613: isc_sha1_update(&hash, (void *)(ent->pool.pool),

Event: ISC library in BIND sources: a HMAC-SHA1 context finalized in function isc_entropy_getdata()
Message: ./fipscc_nios/bind9/lib/isc/entropy.c:615: isc_sha1_final(&hash, digest);

Event: ISC library in BIND sources: macro name
Message: ./fipscc_nios/bind9/lib/isc/entropy.c:620: entropypool_adddata(ent, digest, ISC_SHA1_DIGESTLENGTH, 0);

Event: ISC win32 library in BIND: list of exported functions from libisc has literal "isc_hmacsha1_init" listed
Message: ./fipscc_nios/bind9/lib/isc/win32/libisc.def.in:279:isc_hmacsha1_init

Event: ISC win32 library in BIND: list of exported functions from libisc has literal "isc_hmacsha1_invalidate" listed

Event: ISC win32 library in BIND: list of exported functions from libisc has literal "isc_hmacsha1_sign" listed
Message: ./fipscc_nios/bind9/lib/isc/win32/libisc.def.in:281:isc_hmacsha1_sign

Event: ISC win32 library in BIND: list of exported functions from libisc has literal "isc_hmacsha1_update" listed

Event: ISC win32 library in BIND: list of exported functions from libisc has literal "isc_hmacsha1_verify" listed
Message: ./fipscc_nios/bind9/lib/isc/win32/libisc.def.in:283:isc_hmacsha1_verify

Event: ISC win32 library in BIND: list of exported functions from libisc has literal "isc_sha1_final" listed
Message: ./fipscc_nios/bind9/lib/isc/win32/libisc.def.in:540:isc_sha1_final

Event: ISC win32 library in BIND: list of exported functions from libisc has literal "isc_sha1_init" listed
Message: ./fipscc_nios/bind9/lib/isc/win32/libisc.def.in:541:isc_sha1_init
**Event:** ISC win32 library in BIND: list of exported functions from libisc has literal "isc_sha1_invalidate" listed
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.def.in:542:isc_sha1_invalidate

**Event:** ISC win32 library in BIND: list of exported functions from libisc has literal "isc_sha1_update" listed
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.def.in:543:isc_sha1_update

**Event:** BIND sources, MS libs dev studio project file lists sha1.h
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.dsp.in:550:SOURCE=..\include\isc\sha1.h

**Event:** BIND sources, MS libs dev studio project file lists sha1.c
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.dsp.in:866:SOURCE=..\sha1.c

**Event:** ISC win32 library in BIND: list of library included headers has sha1.h listed
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.vcxproj.filters.in:220:

**Event:** ISC win32 library in BIND: list of library sources includes sha1.c
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.vcxproj.filters.in:615:

**Event:** ISC win32 library in BIND: list of library included headers has sha1.h listed
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.vcxproj.in:336:

**Event:** ISC win32 library in BIND: list of library sources includes sha1.c
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.vcxproj.in:448:

**Event:** Literal in NMAKE file generated from libisc.dsp by MS Studio
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.mak.in:189: -@erase "$(INTDIR)\sha1.obj"

**Event:** Literal in NMAKE file generated from libisc.dsp by MS Studio
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.mak.in:310: "$(INTDIR)\sha1.obj" \n
**Event:** Literal in NMAKE file generated from libisc.dsp by MS Studio
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.mak.in:481: -@erase "$(INTDIR)\sha1.obj"

**Event:** Literal in NMAKE file generated from libisc.dsp by MS Studio
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.mak.in:482: -@erase "$(INTDIR)\sha1.sbr"

**Event:** Literal in NMAKE file generated from libisc.dsp by MS Studio
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.mak.in:620: "$(INTDIR)\sha1.sbr" \n
**Event:** Literal in NMAKE file generated from libisc.dsp by MS Studio
**Message:** .\fipsc_nios\bind9\lib\isc\win32\libisc.mak.in:724: "$(INTDIR)\sha1.obj" $(INTDIR)\sha1.sbr" $(SOURCE) "$($(INTDIR)\sha1.obj" $(INTDIR)\sha1.sbr" $(SOURCE) "$($(INTDIR)"
Event: ISC library in BIND: PKCS11 related macro usage
Message: ./fipscc_nios/bind9/lib/isc/pk11.c:713: rv = pkcs_C_GetMechanismInfo(slot, CKM_SHA1_RSA_PKCS,

Event: ISC library in BIND: PKCS11 related macro usage
Message: ./fipscc_nios/bind9/lib/isc/pk11.c:745: rv = pkcs_C_GetMechanismInfo(slot, CKM_DSA_SHA1, &mechInfo);

Event: BIND Makefile object list
Message: ./fipscc_nios/bind9/lib/isc/Makefile.in:86: safe.@O@ serial.@O@ sha1.@O@ sha2.@O@ sockaddr.@O@ stats.@O@ 

Event: BIND Makefile object list
Message: ./fipscc_nios/bind9/lib/isc/Makefile.in:105: safe.@O@ serial.@O@ sha1.@O@ sha2.@O@ sockaddr.@O@ stats.@O@ 

Event: BIND Makefile sources list
Message: ./fipscc_nios/bind9/lib/isc/Makefile.in:122: safe.c serial.c sha1.c sha2.c sockaddr.c stats.c string.c 

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/isc/iterated_hash.c:23:#include <isc/sha1.h>

Event: ISC library in BIND sources: macro name
Message: ./fipscc_nios/bind9/lib/isc/iterated_hash.c:27:isc_iterated_hash(unsigned char out[ISC_SHA1_DIGESTLENGTH],

Event: ISC library in BIND sources: declaration of a variable of type isc_sha1_t (i.e. EVP_MD_CTX)
Message: ./fipscc_nios/bind9/lib/isc/iterated_hash.c:32:isc_sha1_t ctx;

Event: ISC library in BIND sources: a SHA1 context gets initialized in function isc_iterated_hash()
Message: ./fipscc_nios/bind9/lib/isc/iterated_hash.c:39:isc_sha1_init(&ctx);

Event: ISC library in BIND sources: a SHA1 context gets updated in function isc_iterated_hash()
Message: ./fipscc_nios/bind9/lib/isc/iterated_hash.c:40:isc_sha1_update(&ctx, in, inlength);

Event: ISC library in BIND sources: a SHA1 context gets updated in function isc_iterated_hash()
Message: ./fipscc_nios/bind9/lib/isc/iterated_hash.c:41:isc_sha1_update(&ctx, salt, saltlength);

Event: ISC library in BIND sources: a SHA1 context gets finalized in function isc_iterated_hash()
Message: ./fipscc_nios/bind9/lib/isc/iterated_hash.c:42:isc_sha1_final(&ctx, out);

Event: ISC library in BIND sources: macro name
Message: ./fipscc_nios/bind9/lib/isc/iterated_hash.c:44:inlength = ISC_SHA1_DIGESTLENGTH;

Event: ISC library in BIND sources: macro name
Message: ./fipscc_nios/bind9/lib/isc/iterated_hash.c:47: return (ISC_SHA1_DIGESTLENGTH);

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:671:" CKM_MD2_RSA_PKCS, CKM_MD5_RSA_PKCS, and CKM_SHA1_RSA_PKCS

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:675:#define CKM_SHA1_RSA_PKCS 0x00000006

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:683:" CKM_RSA_X9_31_KEY_PAIR_GEN, CKM_RSA_X9_31, CKM_SHA1_RSA_X9_31,

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:684: " CKM_RSA_PKCS_PSS, and CKM_SHA1_RSA_PKCS_PSS are new for v2.11 */
Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:687:#define CKM_SHA1_RSA_X9_31 0x0000000C

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:689:#define CKM_SHA1_RSA_PKCS_PSS 0x0000000E

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:693:#define CKM_DSA_SHA1 0x00000012

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:888:#define CKM_SSL3_SHA1_MAC 0x00000381

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:891:#define CKM_SHA1_KEY_DERIVATION 0x00000392

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:907:#define CKM_PBE_SHA1_CAST5_CBC 0x000003A5

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:908:#define CKM_PBE_SHA1_CAST128_CBC 0x000003A5

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:909:#define CKM_PBE_SHA1_RC4_128 0x000003A6

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:910:#define CKM_PBE_SHA1_RC4_40 0x000003A7

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:911:#define CKM_PBE_SHA1_DES3_EDE_CBC 0x000003A8

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:912:#define CKM_PBE_SHA1_DES2_EDE_CBC 0x000003A9

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:913:#define CKM_PBE_SHA1_RC2_128_CBC 0x000003AA

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:914:#define CKM_PBE_SHA1_RC2_40_CBC 0x000003AB

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:919:#define CKM_PBA_SHA1_WITH_SHA1_HMAC 0x000003C0

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:1000:#define CKM_ECDSA_SHA1 0x00001042

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:1378:#define CKG_MGF1_SHA1 0x00000001

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:1425:#define CKD_SHA1_KDF 0x00000002

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:1482:#define CKD_SHA1_KDF ASN1 0x00000003

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:1483:#define CKD_SHA1_KDF CONCATENATE 0x00000004
Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/pkcs11/pkcs11t.h:1857:#define CKP_PKCS5_PBD2_HMAC_SHA1 0x00000001

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/isc/include/isc/hmacsha.h:20: * This is the header file for the HMAC-SHA1, HMAC-SHA224, HMAC-SHA256,

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/isc/include/isc/sha1.h:29:#include <isc/sha1.h>

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/isc/include/isc/sha1.h:21:/* $Id: //IB/proj/fipscc_nios/bind9/lib/isc/include/isc/sha1.h#1 $ */

Event: ISC BIND header defines an internal type for HMAC_CTX
Message: ./fipscc_nios/bind9/lib/isc/include/isc/hmacsha.h:42:typedef HMAC_CTX isc_hmacsha1_t;

Event: ISC BIND header defines an internal type for struct pk11_context
Message: ./fipscc_nios/bind9/lib/isc/include/isc/hmacsha.h:51:typedef pk11_context_t isc_hmacsha1_t;

Event: ISC library in BIND sources: declaration of a variable of type isc_sha1_t (i.e. EVP_MD_CTX)
Message: ./fipscc_nios/bind9/lib/isc/include/isc/hmacsha.h:60: isc_sha1_t sha1ctx;

Event: ISC library in BIND: a macro with SHA1 in its name is used as an array length
Message: ./fipscc_nios/bind9/lib/isc/include/isc/hmacsha.h:61: unsigned char key[ISC_HMACSHA1_KEYLENGTH];

Event: ISC library in BIND: a type with name isc_hmacsha1_t is defined
Message: ./fipscc_nios/bind9/lib/isc/include/isc/hmacsha.h:62:} isc_hmacsha1_t;

Event: ISC library in BIND: a function isc_hmacsha1_init() is declared
Message: ./fipscc_nios/bind9/lib/isc/include/isc/hmacsha.h:88:isc_hmacsha1_t *ctx, const unsigned char *key,

Event: ISC library in BIND: a function isc_hmacsha1_invalidate() is declared
Message: ./fipscc_nios/bind9/lib/isc/include/isc/hmacsha.h:92:isc_hmacsha1_t *ctx;

Event: ISC library in BIND: a function isc_hmacsha1_update() is declared
Message: ./fipscc_nios/bind9/lib/isc/include/isc/hmacsha.h:95:isc_hmacsha1_t *ctx, const unsigned char *buf,

Event: ISC library in BIND: a function isc_hmacsha1_sign() is declared
Message: ./fipscc_nios/bind9/lib/isc/include/isc/hmacsha.h:99:isc_hmacsha1_t *ctx, unsigned char *digest, size_t len);

Event: ISC library in BIND: a function isc_hmacsha1_verify() is declared
Message: ./fipscc_nios/bind9/lib/isc/include/isc/hmacsha.h:102:isc_hmacsha1_t *ctx, unsigned char *digest, size_t len);

Event: ISC library in BIND: macro usage
Message: ./fipscc_nios/bind9/lib/isc/include/isc/sha1.h:18:#ifndef ISC_SHA1_H

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/isc/include/isc/sha1.h:19:#define ISC_SHA1_H 1

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/isc/include/isc/sha1.h:21:/* $Id: //IB/proj/fipscc_nios/bind9/lib/isc/include/isc/sha1.h#1 $ */

Event: BIND sources comment

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/isc/include/isc/sha1.h:25:/*!ile isc/sha1.h

Copyright ©2019, Infoblox, Inc. All right reserved.
Event: BIND sources comment
Message:.fipscc_nios/bind9/lib/isc/sha1.c:18:* $Id: //IB/proj/fipscc_nios/bind9/lib/isc/sha1.c#1 $ */

Event: BIND sources comment

Event: BIND sources comment

Event: BIND sources comment
Message:.fipscc_nios/bind9/lib/isc/sha1.c:24: * SHA-1 in C

Event: BIND sources include file named sha1.h
Message:.fipscc_nios/bind9/lib/isc/sha1.c:42:#include <isc/sha1.h>

Event: Function isc_sha1_init definition
Message:.fipscc_nios/bind9/lib/isc/sha1.c:54:isc_sha1_init(isc_sha1_t *context)

Event: Argument of EVP_DigestInit call
Message:.fipscc_nios/bind9/lib/isc/sha1.c:58: RUNTIME_CHECK(EVP_DigestInit(context, EVP_sha1()) == 1);

Event: Function isc_sha1_invalidate definition
Message:.fipscc_nios/bind9/lib/isc/sha1.c:62:isc_sha1_invalidate(isc_sha1_t *context) {

Event: Function isc_sha1_update definition
Message:.fipscc_nios/bind9/lib/isc/sha1.c:67:isc_sha1_update(isc_sha1_t *context, const unsigned char *data,

Event: Function isc_sha1_final definition
Message:.fipscc_nios/bind9/lib/isc/sha1.c:79:isc_sha1_final(isc_sha1_t *context, unsigned char *digest) {

Event: Function isc_sha1_init definition
Message:.fipscc_nios/bind9/lib/isc/sha1.c:89:isc_sha1_init(isc_sha1_t *ctx) {

Event: Function isc_sha1_invalidate definition
Message:.fipscc_nios/bind9/lib/isc/sha1.c:99:isc_sha1_invalidate(isc_sha1_t *ctx) {

Event: Local variables in function isc_sha1_invalidate
Message:.fipscc_nios/bind9/lib/isc/sha1.c:
        100: CK_BYTE garbage[ISC_SHA1_DIGESTLENGTH];
        101: CK_ULONG len = ISC_SHA1_DIGESTLENGTH;

Event: Function isc_sha1_update definition
Message:.fipscc_nios/bind9/lib/isc/sha1.c:111:isc_sha1_update(isc_sha1_t *ctx, const unsigned char *buf, unsigned int len) {

Event: Function isc_sha1_final definition
Message:.fipscc_nios/bind9/lib/isc/sha1.c:121:isc_sha1_final(isc_sha1_t *ctx, unsigned char *digest) {

Event: Local variable in function isc_sha1_final
Message:.fipscc_nios/bind9/lib/isc/sha1.c:123: CK_ULONG len = ISC_SHA1_DIGESTLENGTH;

Event: Comment to macros R0, R1, R2, R3, R4
Message:.fipscc_nios/bind9/lib/isc/sha1.c:155: *(R0+R1), R2, R3, R4 are the different operations (rounds) used in SHA1

Event: Comment to function isc_sha1_init
Message:.fipscc_nios/bind9/lib/isc/sha1.c:315: * isc_sha1_init - Initialize new context
Event: ISC BIND library function to init SHA-1
Message: ./fipscc_nios/bind9/lib/isc/sha1.c:318: isc_sha1_init(isc_sha1_t *context)

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/isc/sha1.c:322: /* SHA1 initialization constants */

Event: Function isc_sha1_invalidate definition
Message: ./fipscc_nios/bind9/lib/isc/sha1.c:333: isc_sha1_invalidate(isc_sha1_t *context) {

Event: Code of function isc_sha1_invalidate
Message: ./fipscc_nios/bind9/lib/isc/sha1.c:334: memset(context, 0, sizeof(isc_sha1_t));

Event: Function isc_sha1_update definition
Message: ./fipscc_nios/bind9/lib/isc/sha1.c:341: isc_sha1_update(isc_sha1_t *context, const unsigned char *data,

Event: Code in function isc_sha1_update
Message: ./fipscc_nios/bind9/lib/isc/sha1.c:
            391: isc_sha1_update(context, &final_0, 1);
            393: isc_sha1_update(context, finalcount, 8);
            402: memset(context, 0, sizeof(isc_sha1_t));

Event: Assign local variable alg in function set_key
Message: ./fipscc_nios/bind9/lib/samples/resolve.c:136: alg = DNS_KEYALG_RSASHA1;

Event: Part of macro algname_is_allocated(algname)
Message: ./fipscc_nios/bind9/lib/dns/tsig.c:81: (algname) != dns_tsig_hmacsha1_name && 

Event: Module variables definition
Message: ./fipscc_nios/bind9/lib/dns/tsig.c:
            133:static unsigned char hmacsha1_ndata[] = "$01hmac-sha1";
            134:static unsigned char hmacsha1_offsets[] = { 0, 10 };

Event: hmacsha1 - instance of struct dns_name
Message: ./fipscc_nios/bind9/lib/dns/tsig.c:
            136:static dns_name_t hmacsha1 = {
            138: hmacsha1_ndata, 11, 2,
            140: hmacsha1_offsets, NULL,

Event: Module variable definition
Message: ./fipscc_nios/bind9/lib/dns/tsig.c:145:LIBDNS_EXTERNAL_DATA dns_name_t *dns_tsig_hmacsha1_name = &hmacsha1;

Event: Code of function ib_dns_tsigkey_createfromkey
Message: ./fipscc_nios/bind9/lib/dns/tsig.c:
            448: } else if (dns_name_equal(algorithm, DNS_TSIG_HMACSHA1_NAME)) {
            449: tkey->algorithm = DNS_TSIG_HMACSHA1_NAME;
            450: if (dstkey != NULL && dst_key_alg(dstkey) != DST_ALG_HMACSHA1) {
Event: Code in function dst_alg_fromname
Message: ./fipscc_nios/bind9/lib/dns/tsig.c:

699: } else if (dns_name_equal(algorithm, DNS_TSIG_HMACSHA1_NAME)) {
700: return (DST_ALG_HMACSHA1);

Event: Code in function dns_tsigkey_create
Message: ./fipscc_nios/bind9/lib/dns/tsig.c:

896: } else if (dns_name_equal(algorithm, DNS_TSIG_HMACSHA1_NAME)) {
902: result = dst_key_frombuffer(name, DST_ALG_HMACSHA1,

Event: Check algorithm type in function dns_tsig_verify
Message: ./fipscc_nios/bind9/lib/dns/tsig.c:1523: if (alg == DST_ALG_HMACMD5 || alg == DST_ALG_HMACSHA1 ||

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/dns/opensslds_link.c:45:#include <isc/sha1.h>

Event: Code of function opensslds_createctx
Message: ./fipscc_nios/bind9/lib/dns/opensslds_link.c:

78: isc_sha1_t *sha1ctx;
82: sha1ctx = isc_mem_get(dctx->mctx, sizeof(isc_sha1_t));
83: isc_sha1_init(sha1ctx);
84: dctx->ctxdata.sha1ctx = sha1ctx;

Event: Code of function opensslds_destroyctx
Message: ./fipscc_nios/bind9/lib/dns/opensslds_link.c:

99: isc_sha1_t *sha1ctx = dctx->ctxdata.sha1ctx;
101: if (sha1ctx != NULL) {
102: isc_sha1_invalidate(sha1ctx);
103: isc_mem_put(dctx->mctx, sha1ctx, sizeof(isc_sha1_t));
104: dctx->ctxdata.sha1ctx = NULL;

Event: Code of function opensslds_adddata
Message: ./fipscc_nios/bind9/lib/dns/opensslds_link.c:

118: isc_sha1_t *sha1ctx = dctx->ctxdata.sha1ctx;
120: isc_sha1_update(sha1ctx, data->base, data->length);

Event: Code of function opensslds_sign
Message: ./fipscc_nios/bind9/lib/dns/opensslds_link.c:

148: isc_sha1_t *sha1ctx = dctx->ctxdata.sha1ctx;
149: unsigned char digest[ISC_SHA1_DIGESTLENGTH];
153: if (r.length < ISC_SHA1_DIGESTLENGTH * 2 + 1)
200: dsasig = DSA_do_sign(digest, ISC_SHA1_DIGESTLENGTH, dsa);
206: isc_sha1_final(sha1ctx, digest);
208: dsasig = DSA_do_sign(digest, ISC_SHA1_DIGESTLENGTH, dsa);
221: BN_bn2bin_fixed(dsasig->r, r.base, ISC_SHA1_DIGESTLENGTH);
222: isc_region_consume(&r, ISC_SHA1_DIGESTLENGTH);
223: BN_bn2bin_fixed(dsasig->s, r.base, ISC_SHA1_DIGESTLENGTH);
224: isc_region_consume(&r, ISC_SHA1_DIGESTLENGTH);
226: isc_buffer_add(sig, ISC_SHA1_DIGESTLENGTH * 2 + 1);

Event: Code of function opensslds_verify
Message: ./fipscc_nios/bind9/lib/dns/opensslds_link.c:

246: isc_sha1_t *sha1ctx = dctx->ctxdata.sha1ctx;
248: unsigned char digest[ISC_SHA1_DIGESTLENGTH];
259: isc_sha1_final(sha1ctx, digest);
262: if (sig->length != 2 * ISC_SHA1_DIGESTLENGTH + 1) {
270:   dsasig->r = BN_bin2bn(cp, ISC_SHA1_DIGESTLENGTH, NULL);
271:   cp += ISC_SHA1_DIGESTLENGTH;
272:   dsasig->s = BN_bin2bn(cp, ISC_SHA1_DIGESTLENGTH, NULL);
294:   status = DSA_do_verify(digest, ISC_SHA1_DIGESTLENGTH, dsasig, dsa);
}

Event: Using ISC_SHA1_DIGESTLENGTH in function opensssldsa_generate
Message: ./fipscc_nios/bind9/lib/dns/opensssldsa_link.c:

360: unsigned char rand_array[ISC_SHA1_DIGESTLENGTH];
402: ISC_SHA1_DIGESTLENGTH, NULL, NULL,
413: ISC_SHA1_DIGESTLENGTH, NULL, NULL,

Event: Using ISC_SHA1_DIGESTLENGTH in function opensssldsa_todns
Message: ./fipscc_nios/bind9/lib/dns/opensssldsa_link.c:

464: dnslen = 1 + (key->key_size * 3)/8 + ISC_SHA1_DIGESTLENGTH;
470: BN_bin2bin_fixed(dsa->q, r.base, ISC_SHA1_DIGESTLENGTH);
471: isc_region_consume(&r, ISC_SHA1_DIGESTLENGTH);

Event: Using ISC_SHA1_DIGESTLENGTH in function opensssldsa_fromdns
Message: ./fipscc_nios/bind9/lib/dns/opensssldsa_link.c:

516: if (r.length < ISC_SHA1_DIGESTLENGTH + 3 * p_bytes) {
521:   dsa->q = BN_bin2bn(r.base, ISC_SHA1_DIGESTLENGTH, NULL);
522:   isc_region_consume(&r, ISC_SHA1_DIGESTLENGTH);
535:   isc_buffer_forward(data, 1 + ISC_SHA1_DIGESTLENGTH + 3 * p_bytes);
}

Event: BIND sources comment

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/dns/validator.c:1828: * need to ignore DNS_DSDIGEST_SHA1 if a DNS_DSDIGEST_SHA256

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/dns/validator.c:1847: digest_types[DNS_DSDIGEST_SHA1] = 0;

Event: BIND sources comment

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/dns/validator.c:2180: * need to ignore DNS_DSDIGEST_SHA1 if a DNS_DSDIGEST_SHA256

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/dns/validator.c:2199: digest_types[DNS_DSDIGEST_SHA1] = 0;

Event: Items of struct parse_map in array map
Message: ./fipscc_nios/bind9/lib/dns/dst_parse.c:

118: [TAG_HMACSHA1_KEY, "Key:'"],
119: [TAG_HMACSHA1_BITS, "Bits:'"],

Event: Cases of switch (alg) in function check_data
Message: ./fipscc_nios/bind9/lib/dns/dst_parse.c:

356: case DST_ALG_RSASHA1:
357: case DST_ALG_NSEC3RSASHA1:
373: case DST_ALG_HMACSHA1:
374: return (check_hmac_sha(priv, HMACSHA1_NTAGS, alg));

Event: Cases of switch (dst_key_alg(key)) in function dst__privstruct_writefile
Message: ./fipscc_nios/bind9/lib/dns/dst_parse.c:

682: case DST_ALG_RSASHA1:
683: fprintf(fp, "(RSASHA1)\n");
685: case DST_ALG_NSEC3RSASHA1:
686: fprintf(fp, "(NSEC3RSASHA1)\n");
709: case DST_ALG_HMACSHA1:
710: fprintf(fp, "(HMAC_SHA1)\n");

Event: Code in function dst__lib_init2
Message: ./fipscc_nios/bind9/lib/dns/dst_api.c:

207: RETERR(dst__hmacsha1_init(&dst_t_func[DST_ALG_HMACSHA1]));
216: RETERR(dst__opensslrsa_init(&dst_t_func[DST_ALG_RSASHA1],
217: DST_ALG_RSASHA1));
218: RETERR(dst__opensslrsa_init(&dst_t_func[DST_ALG_NSEC3RSASHA1],
219: DST_ALG_NSEC3RSASHA1));
239: RETERR(dst__pkcs11rsa_init(&dst_t_func[DST_ALG_RSASHA1]));
240: RETERR(dst__pkcs11rsa_init(&dst_t_func[DST_ALG_NSEC3RSASHA1]));

Event: Code in function dst__ds_digest_supported
Message: ./fipscc_nios/bind9/lib/dns/dst_api.c:

299: return (ISC_TF(digest_type == DNS_DSDIGEST_SHA1 ||
304: return (ISC_TF(digest_type == DNS_DSDIGEST_SHA1 ||

Event: Cases of switch (key->key_alg) in function dst__key_sigsize
Message: ./fipscc_nios/bind9/lib/dns/dst_api.c:

1254: case DST_ALG_RSASHA1:
1255: case DST_ALG_NSEC3RSASHA1:
1276: case DST_ALG_HMACSHA1:
1277: *n = ISC_SHA1_DIGESTLENGTH;

Event: Cases of switch (key->key_alg) in function issymmetric
Message: ./fipscc_nios/bind9/lib/dns/dst_api.c:

1596: case DST_ALG_RSASHA1:
1597: case DST_ALG_NSEC3RSASHA1:

Event: Check algorithm type in function algorithm_status
Message: ./fipscc_nios/bind9/lib/dns/dst_api.c:

1884: if (alg == DST_ALG_RSAMD5 || alg == DST_ALG_RSASHA1 ||
1887: alg == DST_ALG_NSEC3RSASHA1 ||

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/dns/pkcs11dsa_link.c:25:#include <isc/sha1.h>

Event: BIND sources comment
Message: ./fipscc_nios/bind9/lib/dns/pkcs11dsa_link.c:39: * CKM_DSA_SHA1,

Event: Setting local variable mech in function pkcs11dsa_createctx_sign
Message: ./fipscc_nios/bind9/lib/dns/pkcs11dsa_link.c:79: CK_MECHANISM mech = { CKM_DSA_SHA1, NULL, 0 };
Event: Setting local variable mech in function pkcs11dsa_createctx_verify
Message: ./fipscc_nios/bind9/lib/dns/pkcs11dsa_link.c:210: CK_MECHANISM mech = { CKM_DSA_SHA1, NULL, 0 };

Event: Code in function pkcs11dsa_sign
Message: ./fipscc_nios/bind9/lib/dns/pkcs11dsa_link.c:

385: CK_ULONG siglen = ISC_SHA1_DIGESTLENGTH * 2;
392: if (r.length < ISC_SHA1_DIGESTLENGTH * 2 + 1)
398: if (siglen != ISC_SHA1_DIGESTLENGTH * 2)
405: isc_buffer_add(sig, ISC_SHA1_DIGESTLENGTH * 2 + 1);

Event: Code in function pkcs11dsa_todns
Message: ./fipscc_nios/bind9/lib/dns/pkcs11dsa_link.c:

749: dnslen = 1 + (key->key_size * 3)/8 + ISC_SHA1_DIGESTLENGTH;
758: memmove(r.base + ISC_SHA1_DIGESTLENGTH - subprime->ulValueLen,
760: isc_region_consume(&r, ISC_SHA1_DIGESTLENGTH);

Event: Code in function pkcs11dsa_fromdns
Message: ./fipscc_nios/bind9/lib/dns/pkcs11dsa_link.c:

805: if (r.length < ISC_SHA1_DIGESTLENGTH + 3 * p_bytes) {
812: isc_region_consume(&r, ISC_SHA1_DIGESTLENGTH);
825: isc_buffer_forward(data, 1 + ISC_SHA1_DIGESTLENGTH + 3 * p_bytes);
842: attr[1].pValue = isc_mem_get(key->mctx, ISC_SHA1_DIGESTLENGTH);
845: memmove(attr[1].pValue, subprime, ISC_SHA1_DIGESTLENGTH);
846: attr[1].ulValueLen = ISC_SHA1_DIGESTLENGTH;

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:36:#include <isc/sha1.h>

Event: Require Assertion in function opensslrsa_createctx
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:

134: dctx->key->key_alg == DST_ALG_RSASHA1 ||
135: dctx->key->key_alg == DST_ALG_NSEC3RSASHA1 ||

Event: Cases of switch (dctx->key->key_alg) in function opensslrsa_createctx
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:

148: case DST_ALG_RSASHA1:
149: case DST_ALG_NSEC3RSASHA1:
150: type = EVP_sha1(); /* SHA1 + RSA */

Event: Cases of switch (dctx->key->key_alg) in function opensslrsa_createctx
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:

186: case DST_ALG_RSASHA1:
187: case DST_ALG_NSEC3RSASHA1:
189: isc_sha1_t *sha1ctx;
191: sha1ctx = isc_mem_get(dctx->mctx, sizeof(isc_sha1_t));
192: if (sha1ctx == NULL)
194: isc_sha1_init(sha1ctx);
195: dctx->ctxdata.sha1ctx = sha1ctx;

Event: Require Assertion in function opensslrsa_destroyctx
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:

237: dctx->key->key_alg == DST_ALG_RSASHA1 ||
238: dctx->key->key_alg == DST_ALG_NSEC3RSASHA1 ||

Event: Cases of switch (dctx->key->key_alg) in function opensslrsa_destroyctx
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:
   261: case DST_ALG_RSASHA1:
   262: case DST_ALG_NSEC3RSASHA1:
   264: isc_sha1_t *sha1ctx = dctx->ctxdata.sha1ctx;
   266: if (sha1ctx != NULL) {
   267:   isc_sha1_invalidate(sha1ctx);
   268:   isc_mem_put(dctx->mctx, sha1ctx,
   269:   sizeof(isc_sha1_t));
   270:   dctx->ctxdata.sha1ctx = NULL;
   271: }

   Event: Require Assertion in function opensslrsa_adddata
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:
   311: dctx->key->key_alg == DST_ALG_RSASHA1 ||
   312: dctx->key->key_alg == DST_ALG_NSEC3RSASHA1 ||

   Event: Cases of switch (dctx->key->key_alg) in function opensslrsa_adddata
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:
   331: case DST_ALG_RSASHA1:
   332: case DST_ALG_NSEC3RSASHA1:
   334: isc_sha1_t *sha1ctx = dctx->ctxdata.sha1ctx;
   336: isc_sha1_update(sha1ctx, data->base, data->length);
   337: type = NID_sha1;
   338: digestlen = ISC_SHA1_DIGESTLENGTH;

   Event: Require Assertion in function opensslrsa_sign
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:
   397: dctx->key->key_alg == DST_ALG_RSASHA1 ||
   398: dctx->key->key_alg == DST_ALG_NSEC3RSASHA1 ||

   Event: Cases of switch (dctx->key->key_alg) in function opensslrsa_sign
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:
   427: case DST_ALG_RSASHA1:
   428: case DST_ALG_NSEC3RSASHA1:
   430: isc_sha1_t *sha1ctx = dctx->ctxdata.sha1ctx;
   432: isc_sha1_final(sha1ctx, digest);
   433: type = NID_sha1;
   434: digestlen = ISC_SHA1_DIGESTLENGTH;

   Event: Cases of switch (dctx->key->key_alg) in function opensslrsa_sign
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:
   472: case DST_ALG_RSASHA1:
   473: case DST_ALG_NSEC3RSASHA1:

   Event: Require Assertion in function opensslrsa_verify2
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:
   536: dctx->key->key_alg == DST_ALG_RSASHA1 ||
   537: dctx->key->key_alg == DST_ALG_NSEC3RSASHA1 ||

   Event: Cases of switch (dctx->key->key_alg) in function opensslrsa_verify2
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:
   575: case DST_ALG_RSASHA1:
   576: case DST_ALG_NSEC3RSASHA1:
   578: isc_sha1_t *sha1ctx = dctx->ctxdata.sha1ctx;
   580: isc_sha1_final(sha1ctx, digest);
   581: type = NID_sha1;
   582: digestlen = ISC_SHA1_DIGESTLENGTH;
Event: Cases of switch (dctx->key->key_algorithm) in function opensslrsa_verify2
Message: ./fipscc_nios/bind9/lib/dns/opensslrsa_link.c:
   623: case DST_ALG_RSASHA1:
   624: case DST_ALG_NSEC3RSASHA1:

Event: Code in function compute_cc
Message: ./fipscc_nios/bind9/lib/dns/resolver.c:
   2318:#ifdef HMAC_SHA1_SIT
   2319: unsigned char digest[ISC_SHA1_DIGESTLENGTH];
   2321: isc_hmacsha1_t hmacsha1;
   2323: isc_hmacsha1_init(&hmacsha1, query->fctx->res->view->secret,
   2325: ISC_SHA1_DIGESTLENGTH);
   2330: isc_hmacsha1_update(&hmacsha1,
   2332: isc_hmacsha1_update(&hmacsha1,
   2334: isc_hmacsha1_update(&hmacsha1,
   2338: isc_hmacsha1_sign(&hmacsha1, digest, sizeof(digest));
   2340: isc_hmacsha1_invalidate(&hmacsha1);

Event: Case of switch (dst_key_algorithm(key)) in function dns_tsec_create
Message: ./fipscc_nios/bind9/lib/dns/tsec.c:
   71: case DST_ALG_HMACSHA1:
   72: algname = dns_tsig_hmacsha1_name;

Event: Check and set algorithm type in function zone_check_dnskeys
Message: ./fipscc_nios/bind9/lib/dns(zone.c):
   5247: if ((dnskey.algorithm == DST_ALG_RSASHA1 ||
   5252: if (dnskey.algorithm == DST_ALG_RSASHA1) {
   5255: algorithm = "RSASHA1";

Event: Check algorithm type in function dnskey_sane
Message: ./fipscc_nios/bind9/lib/dns(zone.c:21643: if (alg == DST_ALG_RSAMD5 || alg == DST_ALG_RSASHA1 ||

Event: Check algorithm type in function dns_nsec_nseconly
Message: ./fipscc_nios/bind9/lib/dns/nsec.c:249: dnskey.algorithm == DST_ALG_RSASHA1 ||

Event: Items of enum gssd_etype_t
Message: ./fipscc_nios/bind9/lib/dns/infoblox_gssdiag_counters.h:
   16: GSSD_ETYPE_AES128_CTS_HMAC_SHA1_96,
   17: GSSD_ETYPE_AES256_CTS_HMAC_SHA1_96,

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/dns/ds.c:28:#include <isc/sha1.h>

Event: Type dst_hmacsha1_key_t definition
Message: ./fipscc_nios/bind9/lib/dns/dst_internal.h:81:typedef struct dst_hmacsha1_key dst_hmacsha1_key_t;

Event: Field in struct dst_key
Message: ./fipscc_nios/bind9/lib/dns/dst_internal.h:125: dst_hmacsha1_key_t *hmacsha1;

Event: Fields of union ctxdata in struct dst_context
Message: ./fipscc_nios/bind9/lib/dns/dst_internal.h:
   158: isc_sha1_t *sha1ctx;
   162: isc_hmacsha1_t *hmacsha1ctx;

Event: dst__hmacsha1_init function declaration
Message: ./fipscc_nios/bind9/lib/dns/dst_internal.h:228:isc_result_t dst__hmacsha1_init(struct dst_func **funcp);

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/dns/ds.c:28:#include <isc/sha1.h>

Event: Local variable in function dns_ds_buildrdata
Message:  ./fipscc_nios/bind9/lib/dns/ds.c:56: isc_sha1_t sha1;

Event: Case of switch (digest_type) in function dns_ds_buildrdata
Message:  ./fipscc_nios/bind9/lib/dns/ds.c:

77: case DNS_DSDIGEST_SHA1:
78: isc_sha1_init(&sha1);
80: isc_sha1_update(&sha1, r.base, r.length);
83: isc_sha1_update(&sha1, r.base, r.length);
84: isc_sha1_final(&sha1, digest);

Event: Case of switch (digest_type) in function dns_ds_buildrdata
Message:  ./fipscc_nios/bind9/lib/dns/ds.c:

136: case DNS_DSDIGEST_SHA1:
137: ds.length = ISC_SHA1_DIGESTLENGTH;

Event: BIND sources comment
Message:  ./fipscc_nios/bind9/lib/dns/dst_parse.h:54:/* These are used by both RSA-MD5 and RSA-SHA1 */

Event: BIND sources macro definition
Message:  ./fipscc_nios/bind9/lib/dns/dst_parse.h:94:#define HMACSHA1_NTAGS 2

Event: BIND sources macro definition
Message:  ./fipscc_nios/bind9/lib/dns/dst_parse.h:95:#define TAG_HMACSHA1_KEY ((DST_ALG_HMACSHA1 << TAG_SHIFT) + 0)

Event: BIND sources macro definition
Message:  ./fipscc_nios/bind9/lib/dns/dst_parse.h:96:#define TAG_HMACSHA1_BITS ((DST_ALG_HMACSHA1 << TAG_SHIFT) + 1)

Event: BIND sources macro definition
Message:  ./fipscc_nios/bind9/lib/dns/rcode.c:109: { DNS_KEYALG_RSASHA1, "RSASHA1", 0 }, \

Event: BIND sources macro definition
Message:  ./fipscc_nios/bind9/lib/dns/rcode.c:110: { DNS_KEYALG_NSEC3RSASHA1, "NSEC3RSASHA1", 0 }, \

Event: BIND sources macro definition
Message:  ./fipscc_nios/bind9/lib/dns/rcode.c:133: { 1, "SHA-1", 0 }, \

Event: BIND sources macro definition
Message:  ./fipscc_nios/bind9/lib/dns/rcode.c:139: { DNS_DSDIGEST_SHA1, "SHA-1", 0 }, \

Event: Cases of switch(tsd->etype) in function gssd_format_crypto
Message:  ./fipscc_nios/bind9/lib/dns/infoblox_gssdiag.c:

256: case ETYPE_AES128_CTS_HMAC_SHA1_96: etype = "aes128-cts-hmac-sha1-96"; break;
257: case ETYPE_AES256_CTS_HMAC_SHA1_96: etype = "aes256-cts-hmac-sha1-96"; break;

Event: Cases of switch(tsd->etype) in function gssd_end_reporting
Message:  ./fipscc_nios/bind9/lib/dns/infoblox_gssdiag.c:

329: GSSD_ETYPE(ETYPE_AES128_CTS_HMAC_SHA1_96);
330: GSSD_ETYPE(ETYPE_AES256_CTS_HMAC_SHA1_96);

Event: BIND sources include file named sha1.h
Message:  ./fipscc_nios/bind9/lib/dns/pkcs11rsa_link.c:25:#include <isc/sha1.h>

Event: Require Assertion in function pkcs11rsa_createctx_sign
Message:  ./fipscc_nios/bind9/lib/dns/pkcs11rsa_link.c:

87: key->key_alg == DST_ALG_RSASHA1 ||
88: key->key_alg == DST_ALG_NSEC3RSASHA1 ||
Event: Cases of switch (dctx->key->key_alg) in function pkcs11rsa_createctx_sign
Message: ./fipscc_nios/bind9/lib/dns/pkcs11rsa_link.c:
   213: case DST_ALG_RSASHA1:
   214: case DST_ALG_NSEC3RSASHA1:
   215: mech.mechanism = CKM_SHA1_RSA_PKCS;

Event: Require Assertion in function pkcs11rsa_createctx_verify
Message: ./fipscc_nios/bind9/lib/dns/pkcs11rsa_link.c:
   287: key->key_alg == DST_ALG_RSASHA1 ||
   288: key->key_alg == DST_ALG_NSEC3RSASHA1 ||

Event: Cases of switch (dctx->key->key_alg) in function pkcs11rsa_createctx_verify
Message: ./fipscc_nios/bind9/lib/dns/pkcs11rsa_link.c:
   345: case DST_ALG_RSASHA1:
   346: case DST_ALG_NSEC3RSASHA1:
   347: mech.mechanism = CKM_SHA1_RSA_PKCS;

Event: Case of switch (hashalg) in function dns_nsec3_buildrdata
Message: ./fipscc_nios/bind9/lib/dns/nsec3.c:
   92: case dns_hash_sha1:
   93: REQUIRE(hash_length == ISC_SHA1_DIGESTLENGTH);

Event: Case of switch (hash) in function dns_nsec3_hashlength
Message: ./fipscc_nios/bind9/lib/dns/nsec3.c:
   285: case dns_hash_sha1:
   286: return(ISC_SHA1_DIGESTLENGTH);

Event: Case of switch (hash) in function dns_nsec3_supportedhash
Message: ./fipscc_nios/bind9/lib/dns/nsec3.c:294: case dns_hash_sha1:

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/dns/hmac_link.c:43:#include <isc/sha1.h>

Event: Function hmacsha1_frommdns declaration
Message: ./fipscc_nios/bind9/lib/dns/hmac_link.c:350:static isc_result_t hmacsha1_frommdns(dst_key_t *key, isc_buffer_t *data);

Event: struct dst_hmacsha1_key definition
Message: ./fipscc_nios/bind9/lib/dns/hmac_link.c:
   352:struct dst_hmacsha1_key {
   353: unsigned char key[ISC_SHA1_BLOCK_LENGTH];

Event: Code of function hmacsha1_createctx
Message: ./fipscc_nios/bind9/lib/dns/hmac_link.c:
   357:hmacsha1_createctx(dst_key_t *key, dst_context_t *dctx) {
   358: isc_hmacsha1_t *hmacsha1ctx;
   359: dst_hmacsha1_key_t *hkey = key->keydata.hmacsha1;
   361: hmacsha1ctx = isc_mem_get(dctx->mctx, sizeof(isc_hmacsha1_t));
   362: if (hmacsha1ctx == NULL)
   364: isc_hmacsha1_init(hmacsha1ctx, hkey->key, ISC_SHA1_BLOCK_LENGTH);
   365: dctx->ctxdata.hmacsha1ctx = hmacsha1ctx;

Event: Code of function hmacsha1_destroyctx
Message: ./fipscc_nios/bind9/lib/dns/hmac_link.c:
   370:hmacsha1_destroyctx(dst_context_t *dctx) {
   371: isc_hmacsha1_t *hmacsha1ctx = dctx->ctxdata.hmacsha1ctx;
   373: if (hmacsha1ctx != NULL) {
   374: isc_hmacsha1_invalidate(hmacsha1ctx);
   375: isc_mem_put(dctx->mctx, hmacsha1ctx, sizeof(isc_hmacsha1_t));
   376: dctx->ctxdata.hmacsha1ctx = NULL;

Event: Code of function hmacsha1_adddata
hmacsha1_adddata(dst_context_t *dctx, const isc_region_t *data) {
    isc_hmacsha1_t *hmacsha1ctx = dctx->ctxdata.hmacsha1ctx;
    isc_hmacsha1_update(hmacsha1ctx, data->base, data->length);
}

hmacsha1_sign(dst_context_t *dctx, isc_buffer_t *sig) {
    isc_hmacsha1_t *hmacsha1ctx = dctx->ctxdata.hmacsha1ctx;
    if (isc_buffer_availablelength(sig) < ISC_SHA1_DIGESTLENGTH)
        hmacsha1_sign(hmacsha1ctx, digest, ISC_SHA1_DIGESTLENGTH);
    isc_buffer_add(sig, ISC_SHA1_DIGESTLENGTH);
}

hmacsha1_verify(dst_context_t *dctx, const isc_region_t *sig) {
    isc_hmacsha1_t *hmacsha1ctx = dctx->ctxdata.hmacsha1ctx;
    if (sig->length > ISC_SHA1_DIGESTLENGTH || sig->length == 0)
        hmacsha1_verify(hmacsha1ctx, sig->base, sig->length);
}

hmacsha1_compare(const dst_key_t *key1, const dst_key_t *key2) {
    dst_hmacsha1_key_t *hkey1, *hkey2;
    hkey1 = key1->keydata.hmacsha1;
    hkey2 = key2->keydata.hmacsha1;
    if (isc_safe_memequal(hkey1->key, hkey2->key, ISC_SHA1_BLOCK_LENGTH))
}

hmacsha1_generate(dst_key_t *key, int pseudorandom_ok, void (*callback)(int)) {
    unsigned char data[ISC_SHA1_BLOCK_LENGTH];
    if (bytes > ISC_SHA1_BLOCK_LENGTH) {
        bytes = ISC_SHA1_BLOCK_LENGTH;
        key->keysize = ISC_SHA1_BLOCK_LENGTH * 8;
        memset(data, 0, ISC_SHA1_BLOCK_LENGTH);
    }
    ret = hmacsha1_fromdns(key, &data);
    memset(data, 0, ISC_SHA1_BLOCK_LENGTH);
}

hmacsha1_isprivate(const dst_key_t *key) {
}

hmacsha1_destroy(dst_key_t *key) {
    dst_hmacsha1_key_t *hkey = key->keydata.hmacsha1;
    memset(hkey, 0, sizeof(dst_hmacsha1_key_t));
    isc_mem_put(key->mctx, hkey, sizeof(dst_hmacsha1_key_t));
    key->keydata.hmacsha1 = NULL;
}

hmacsha1_todns(const dst_key_t *key, isc_buffer_t *data) {
    dst_hmacsha1_key_t *hkey;
    REQUIRE(key->keydata.hmacsha1 != NULL);
    hkey = key->keydata.hmacsha1;
}

hmacsha1_fromdns
495: hmacsha1_fromdns(dst_key_t *key, isc_buffer_t *data) {
496: dst_hmacsha1_key_t *hkey;
499: isc_sha1_t sha1ctx;
505: hkey = isc_mem_get(key->mctx, sizeof(dst_hmacsha1_key_t));
511: if (r.length > ISC_SHA1_BLOCK_LENGTH) {
512: isc_sha1_init(&sha1ctx);
513: isc_sha1_update(&sha1ctx, r.base, r.length);
514: isc_sha1_final(&sha1ctx, hkey->key);
515: keylen = ISC_SHA1_DIGESTLENGTH;
522: key->keydata.hmacsha1 = hkey;

Event: Code of function hmacsha1_tofile
Message: ./fipscc_nios/bind9/lib/dns/hmac_link.c:

530: hmacsha1_tofile(const dst_key_t *key, const char *directory) {
532: dst_hmacsha1_key_t *hkey;
537: if (key->keydata.hmacsha1 == NULL)
543: hkey = key->keydata.hmacsha1;
545: priv.elements[cnt].tag = TAG_HMACSHA1_KEY;
551: priv.elements[cnt].tag = TAG_HMACSHA1_BITS;

Event: Code of function hmacsha1_parse
Message: ./fipscc_nios/bind9/lib/dns/hmac_link.c:

560: hmacsha1_parse(dst_key_t *key, isc_lex_t *lexer, dst_key_t *pub) {
569: result = dst__privstruct_parse(key, DST_ALG_HMACSHA1, lexer, mctx,
580: case TAG_HMACSHA1_KEY:
584: tresult = hmacsha1_fromdns(key, &b);
588: case TAG_HMACSHA1_BITS:

Event: hmacsha1_functions - instance of struct dst_func_t /* Context functions */
Message: ./fipscc_nios/bind9/lib/dns/hmac_link.c:

603: static dst_func_t hmacsha1_functions = {
604: hmacsha1_createctx,
606: hmacsha1_destroyctx,
607: hmacsha1_adddata,
608: hmacsha1_sign,
609: hmacsha1_verify,
612: hmacsha1_compare,
614: hmacsha1_generate,
615: hmacsha1_isprivate,
616: hmacsha1_destroy,
617: hmacsha1_todns,
618: hmacsha1_fromdns,
619: hmacsha1_tofile,
620: hmacsha1_parse,

Event: Code of function dst__hmacsha1_init
Message: ./fipscc_nios/bind9/lib/dns/hmac_link.c:

628: dst__hmacsha1_init(dst_func_t **funcp) {
631: *funcp = &hmacsha1_functions;

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/dns/rdata/generic/dlv_32769.c:26:#include <isc/sha1.h>

Event: Case of switch (c) /*Digest*/ in function fromtext_dlv
Message: ./fipscc_nios/bind9/lib/dns/rdata/generic/dlv_32769.c:

79: case DNS_DSDIGEST_SHA1:
80: length = ISC_SHA1_DIGESTLENGTH;

Event: Check and copy digest lengths if we know them in function fromwire_dlv
Message: ./fipscc_nios/bind9/lib/dns/rdata/generic/dlv_32769.c:
173: (sr.base[3] == DNS_DSDIGEST_SHA1 &&
174: sr.length < 4 + ISC_SHA1_DIGESTLENGTH) ||
190: if (sr.base[3] == DNS_DSDIGEST_SHA1)
191: sr.length = 4 + ISC_SHA1_DIGESTLENGTH;

Event: Case of switch (dlv->digest_type) in function fromstruct_dlv
Message: ./fipscc_nios/bind9/lib/dns/data/generic/dlv_32769.c:

243: case DNS_DSDIGEST_SHA1:
244: REQUIRE(dlv->length == ISC_SHA1_DIGESTLENGTH);

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/dns/data/generic/cds_59.c:24:#include <isc/sha1.h>

Event: Case of switch (c) in function fromtext_cds
Message: ./fipscc_nios/bind9/lib/dns/data/generic/cds_59.c:

74: case DNS_DSDIGEST_SHA1:
75: length = ISC_SHA1_DIGESTLENGTH;

Event: Check and copy digest lengths if we know them in function fromwire_cds
Message: ./fipscc_nios/bind9/lib/dns/data/generic/cds_59.c:

168: (sr.base[3] == DNS_DSDIGEST_SHA1 &&
169: sr.length < 4 + ISC_SHA1_DIGESTLENGTH) ||
185: if (sr.base[3] == DNS_DSDIGEST_SHA1)
186: sr.length = 4 + ISC_SHA1_DIGESTLENGTH;

Event: Case of switch (ds->digest_type) in function fromstruct_cds
Message: ./fipscc_nios/bind9/lib/dns/data/generic/cds_59.c:

238: case DNS_DSDIGEST_SHA1:
239: REQUIRE(ds->length == ISC_SHA1_DIGESTLENGTH);

Event: Require Assertion
Message: ./fipscc_nios/bind9/lib/dns/data/generic/nsec3_50.c:357: REQUIRE(nsec3->hash == dns_hash_sha1);

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/lib/dns/data/generic/ds_43.c:28:#include <isc/sha1.h>

Event: Case of switch (c) in function fromtext_ds
Message: ./fipscc_nios/bind9/lib/dns/data/generic/ds_43.c:

78: case DNS_DSDIGEST_SHA1:
79: length = ISC_SHA1_DIGESTLENGTH;

Event: Check and copy digest lengths if we know them in function fromwire_ds
Message: ./fipscc_nios/bind9/lib/dns/data/generic/ds_43.c:

172: (sr.base[3] == DNS_DSDIGEST_SHA1 &&
173: sr.length < 4 + ISC_SHA1_DIGESTLENGTH) ||
189: if (sr.base[3] == DNS_DSDIGEST_SHA1)
190: sr.length = 4 + ISC_SHA1_DIGESTLENGTH;

Event: Case of switch (ds->digest_type) in function fromstruct_ds
Message: ./fipscc_nios/bind9/lib/dns/data/generic/ds_43.c:

242: case DNS_DSDIGEST_SHA1:
243: REQUIRE(ds->length == ISC_SHA1_DIGESTLENGTH);

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/dns/include/dst/dst.h:59:#define DST_ALG_RSASHA1 5
Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/dns/include/dst/dst.h:61:#define DST_ALG_NSEC3RSASHA1 7

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/dns/include/dst/dst.h:69:#define DST_ALG_HMACSHA1 161 /* XXXMPA */

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/dns/include/dns/ds.h:27:#define DNS_DSDIGEST_SHA1 (1)

Event: BIND sources: part (name dns_hash_sha1) of enumerated type dns_hash_t being defined
Message: ./fipscc_nios/bind9/lib/dns/include/dns/types.h:170: dns_hash_sha1 = 1

Event: BIND sources comment

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/dns/include/dns/keyvalues.h:69:#define DNS_KEYALG_RSASHA1 5

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/dns/include/dns/keyvalues.h:70:#define DNS_KEYALG_NSEC3RSASHA1 7

Event: BIND sources: external type declaration
Message: ./fipscc_nios/bind9/lib/dns/include/dns/tsig.h:45:LIBDNS_EXTERNAL_DATA extern dns_name_t *dns_tsig_hmacsha1_name;

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/lib/dns/include/dns/tsig.h:46:#define DNS_TSIG_HMACSHA1_NAME dns_tsig_hmacsha1_name

Event: BIND sources comment
Message: ./fipscc_nios/bind9/config.h.in:467:/" Use HMAC-SHA1 for Source Identity Token generation */

Event: BIND sources: clear definition of HMAC_SHA1_SIT
Message: ./fipscc_nios/bind9/config.h.in:468:#undef HMAC_SHA1_SIT

Event: BIND sources comment
Message: ./fipscc_nios/bind9/config.h.win32:366:/* Use HMAC-SHA1 for Source Identity Token generation */

Event: BIND sources: literal in Win32 configuration file
Message: ./fipscc_nios/bind9/config.h.win32:367:@HMAC_SHA1_SIT@

Event: BIND configure script argument help
Message: ./fipscc_nios/bind9/configure.in:1377: [ --with-sit-alg=ALG choose the algorithm for SIT [[aes|sha1|sha256]]],

Event: BIND configure script internal variable set with "sha-1" literal
Message: ./fipscc_nios/bind9/configure.in:1384: with_sit_alg="sha1"

Event: BIND configure script internal variable value check
Message: ./fipscc_nios/bind9/configure.in:1845: sha1)
Event: BIND configure script parameter set
Message: ./fipscc_nios/bind9/configure.in:1850: AC_MSG_RESULT(sha1)

Event: BIND configure script parameter definition
Message: ./fipscc_nios/bind9/configure.in:1858: AC_DEFINE(HMAC_SHA1_SIT, 1,

Event: BIND configure script parameter definition
Message: ./fipscc_nios/bind9/configure.in:1859: [Use HMAC-SHA1 for Source Identity Token generation]

Event: BIND configure script help string
Message: ./fipscc_nios/bind9/win32utils/Configure:369: "HMAC_SHA1_SIT", literal

Event: BIND configure script help literal
Message: ./fipscc_nios/bind9/win32utils/Configure:556:" with-sit-alg choose the algorithm for SIT aes|sha1|sha256 in",

Event: BIND configure script literal in IF-statement to define the configuration
Message: ./fipscc_nios/bind9/win32utils/Configure:1865: if ($sit_algorithm eq "sha1") {

Event: BIND configure script literal in IF-statement to define the configuration
Message: ./fipscc_nios/bind9/win32utils/Configure:1866: $configdefh{"HMAC_SHA1_SIT"} = 1;

Event: BIND documentation
Message: ./fipscc_nios/bind9/doc/rfc/index:70:3110: RSA/SHA-1 SIGs and RSA KEYS in the Domain Name System (DNS)

Event: BIND documentation
Message: ./fipscc_nios/bind9/doc/misc/SIT:73:HMAC SHA1

Event: BIND documentation
Message: ./fipscc_nios/bind9/doc/misc/SIT:75: hash = trunc(hmacsha1(secret, client|nonce|when|address), 8);

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/contrib/dnsperf-2.1.0.0-1/dns.c:79:#define TSIG_HMACSHA1_NAME "

Event: Item of enum hmac_type_t
Message: ./fipscc_nios/bind9/contrib/dnsperf-2.1.0.0-1/dns.c:87: TSIG_HMACSHA1,

Event: Item of union hmac_ctx_t
Message: ./fipscc_nios/bind9/contrib/dnsperf-2.1.0.0-1/dns.c:96: isc_hmacsha1_t hmacsha1;

Event: Check algorithm type and set key in function perf_dns_parsetsigkey
Message: ./fipscc_nios/bind9/contrib/dnsperf-2.1.0.0-1/dns.c:
        244: } else if (strncasecmp(alg, "hmac-sha1:", 10) == 0) {
        245: SET_KEY(tsigkey, SHA1);

Event: Case of switch (tsigkey->hmactype) in function hmac_init
Message: ./fipscc_nios/bind9/contrib/dnsperf-2.1.0.0-1/dns.c:
        342: case TSIG_HMACSHA1:
        343: isc_hmacsha1_init(&ctx->hmacsha1, secret, length);

Event: Case of switch (tsigkey->hmactype) in function hmac_update
Message: ./fipscc_nios/bind9/contrib/dnsperf-2.1.0.0-1/dns.c:
        368: case TSIG_HMACSHA1:
        369: isc_hmacsha1_update(&ctx->hmacsha1, data, length);

Event: Case of switch (tsigkey->hmactype) in function hmac_sign
Message: ./fipscc_nios/bind9/contrib/dnsperf-2.1.0.0-1/dns.c:

    394: case TSIG_HMACSHA1:
    395: isc_hmacsha1_sign(&ctx->hmacsha1_sign,&ctx->hmacsha1,digest,digestlen);

Event: BIND sources comment
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/zconf.h:70/* # define KSK_ALGO (DK_ALGO_RSASHA1) KSK_ALGO renamed to KEY_ALGO (v0.99) */

Event: BIND sources comment
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/zconf.h:71:/* # define KEY_ALGO (DK_ALGO_RSASHA1) */ general KEY_ALGO used for both ksk and zsk */

Event: BIND sources comment
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/zconf.h:75:/* # define ZSK_ALGO (DK_ALGO_RSASHA1) ZSK_ALGO has to be the same as KSK, so this is no longer used (v0.99) */

Event: Check algorithm type in function dki_new which creates new keyfile
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/dki.c:255: if ( algo == DK_ALGO_RSA || algo == DK_ALGO_RSASHA1 || algo ==

Event: Cases of switch ( algo ) in function dki_algo2str which returns a string describing the key algorithm
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/dki.c:632: case DK_ALGO_RSASHA1: return ("RSASHA1");
634: case DK_ALGO_NSEC3RSASHA1: return ("NSEC3RSASHA1");

Event: Cases of switch ( algo ) in function dki_algo2sstr which returns a short string describing the key algorithm
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/dki.c:

    653: case DK_ALGO_RSASHA1: return ("RSASHA1");
    655: case DK_ALGO_NSEC3RSASHA1: return ("N3RSA1");

Event: Code in function genkey which generates a DNSKEY key
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/rollover.c:

    103: if (config algo == DK_ALGO_RSASHA1)
    104: algo = DK_ALGO_NSEC3RSASHA1;

Event: Code in case CONF_ALGO of switch ( c->type ) in function parseconfigline
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/zconf.c:

    430: strcasecmp (val, "rsasha1") == 0 )
    431: *((int *)c->var) = DK_ALGO_RSASHA1;
    437: strcasecmp (val, "nsec3rsasha1") == 0 ||
    438: strcasecmp (val, "n3rsasha1") == 0 )
    439: *((int *)c->var) = DK_ALGO_NSEC3RSASHA1;

Event: BIND dnssec config example

Event: BIND dnssec config example
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/examples/views/dnssec-intern.conf:26:ZSK_algo: RSASHA1 # (Algorithm ID 5)

Event: BIND dnssec config example

Event: BIND dnssec config example
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/examples/views/dnssec-extern.conf:26:ZSK_algo: RSASHA1 # (Algorithm ID 5)

Event: BIND dnssec config example
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/examples/hierarchical/de/example.de/sub.example.de/dnssec.conf:10:Key_algo RSASHA1

Event: BIND dnssec config example
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/examples/hierarchical/de/example.de/sub.example.de/dnssec.conf:21:Key_Algo: RSASHA1 # (Algorithm ID 5)

Event: Comment in BIND dnssec zone key tool example
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/examples/flat/sub.example.net/zone.db.signed:39: ) ; ZSK; alg = NSEC3RSASHA1; key id = 6419

Copyright ©2019, Infoblox, Inc. All right reserved.
Event: Comment in BIND dnssec zone key tool example
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/examples/flat/sub.example.net/zone.db.signed:60: ) ; KSK; alg = NSEC3RSASHA1; key id = 33936

Event: Comment in BIND dnssec zone key tool example
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/examples/flat/sub.example.net/dnskey.db:17:; sub.example.net. tag=33936 algo=NSEC3RSASHA1 generated Nov 14 2014 18:11:13

Event: Comment in BIND dnssec zone key tool example
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/examples/flat/sub.example.net/dnskey.db:34:; sub.example.net. tag=6419 algo=NSEC3RSASHA1 generated Nov 14 2014 18:11:13

Event: Comment in BIND dnssec zone key tool example
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/examples/flat/keysets/keyset-sub.example.net.:8: ) ; KSK; alg = NSEC3RSASHA1; key id = 33936

Event: BIND dnssec zone key tool config example
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/examples/flat/dyn.example.net/dnssec.conf:1:Key_Algo: NSEC3RSASHA1 # (Algorithm ID 7)

Event: BIND sources: in the function sign_zone(): a macro usage which has SHA1 in its name to determine configured algorithm in if block
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/zkt-signer.c:883: if ( conf->k_algo == DK_ALGO_NSEC3DSA || conf->k_algo == DK_ALGO_NSEC3RSASHA1 ||

Event: BIND dnssec zone key tool changelog
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/CHANGELOG:61:* bug If nsec3 is turned on and KeyAlgo (or AddKeyAlgo) is RSHASHA1

Event: BIND dnssec zone key tool changelog
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/CHANGELOG:62: or DSA, genkey() uses algorithm type NSECRSASHA1 or NSEC3DSA instead.

Event: BIND dnssec zone key tool sources define
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/dki.h:62:# define DK_ALGO_RSASHA1 5 /* RFC3110 */

Event: BIND dnssec zone key tool sources define
Message: ./fipscc_nios/bind9/contrib/zkt-1.1.3/dki.h:64:# define DK_ALGO_NSEC3RSASHA1 7 /* symlink to alg 5 RFC5155 */

Event: BIND configure script help
Message: ./fipscc_nios/bind9/configure:1765: --with-sit-alg=ALG choose the algorithm for SIT [aes|sha1|sha256]

Event: BIND configure script
Message: ./fipscc_nios/bind9/configure:19940: with_sit_alg="sha1"

Event: BIND configure script literal
Message: ./fipscc_nios/bind9/configure:20970: sha1)

Event: BIND configure script literal
Message: ./fipscc_nios/bind9/configure:20977: [ $as_echo "$as_me:$LINENO: result: sha1" >&5

Event: BIND configure script literal
Message: ./fipscc_nios/bind9/configure:20978:$as_echo "sha1" >&6; }

Event: BIND configure script define
Message: ./fipscc_nios/bind9/configure:20988:#define HMAC_SHA1_SIT 1

Event: BIND changelog
Message: ./fipscc_nios/bind9/CHANGES:1943:3562. [func] Update map file header format to include a SHA-1 hash

Event: BIND changelog
Event: BIND changelog

Event: BIND changelog
Message: ./fipscc_nios/bind9/CHANGES:3334: for the hashing algorithms (md5, sha1 - sha512,

Event: BIND changelog
Message: ./fipscc_nios/bind9/CHANGES:4837: (i.e., RSASHA1, or NSEC3RSASHA1 if -3 is used).

Event: BIND changelog
Message: ./fipscc_nios/bind9/CHANGES:5164: generate a 1024-bit RSASHA1 zone-signing key,

Event: BIND changelog
Message: ./fipscc_nios/bind9/CHANGES:5165: or with the -f KSK option, a 2048-bit RSASHA1

Event: BIND changelog
Message: ./fipscc_nios/bind9/CHANGES:6425:2215. [bug] Bad REQUIRE check isc_hmacsha1_verify(). [RT #17094]

Event: BIND changelog

Event: BIND changelog

Event: Code in function parse_hmac which parses HMAC algorithm specification
Message: ./fipscc_nios/bind9/bin/dig/dighost.c:

```c
1196: } else if (strcasecmp(buf, "hmac-sha1") == 0) {
1197: hmacname = DNS_TSIG_HMACSHA1_NAME;
1199: } else if (strncasecmp(buf, "hmac-sha1-", 10) == 0) {
1200: hmacname = DNS_TSIG_HMACSHA1_NAME;
```

Event: Case of switch (dst_key_alg(dstkey)) in function setup_file_key
Message: ./fipscc_nios/bind9/bin/dig/dighost.c:

```c
1312: case DST_ALG_HMACSHA1:
1313: hmacname = DNS_TSIG_HMACSHA1_NAME;
```

Event: BIND sources include file named sha1.h
Message: ./fipscc_nios/bind9/bin/tools/isc-hmac-fixup.c:26:#include <isc/sha1.h>

Event: Part of usage code in function main
Message: ./fipscc_nios/bind9/bin/tools/isc-hmac-fixup.c:44: fprintf(stderr, "talgorithm: (MD5 | SHA1 | SHA224 | "

Event: Code in function main
Message: ./fipscc_nios/bind9/bin/tools/isc-hmac-fixup.c:

```c
68: } else if (!strcasecmp(argv[1], "sha1") ||
69: !strcasecmp(argv[1], "hmac-sha1") ||
70: if (r.length > ISC_SHA1_DIGESTLENGTH) {
71: isc_sha1_f sha1ctx;
72: isc_sha1_init(&sha1ctx);
73: isc_sha1_update(&sha1ctx, r.base, r.length);
74: isc_sha1_final(&sha1ctx, key);
77: r.length = ISC_SHA1_DIGESTLENGTH;
```

Event: BIND documentation
Message: ./fipscc_nios/bind9/bin/tools/nsec3hash.docbook:80: only supported hash algorithm for NSEC3 is SHA-1,

Event: BIND documentation
Message: ./fipscc_nios/bind9/bin/tools/isc-hmac-fixup.docbook:58: hash algorithm (i.e., SHA1 keys longer than 160 bits, SHA256 keys
38:Versions of BIND 9 up to and including BIND 9.6 had a bug causing HMAC-SHA* TSIG keys which were longer than the digest length of the hash algorithm (i.e., SHA1 keys longer than 160 bits, SHA256 keys longer than 256 bits, etc) to be used incorrectly, generating a message authentication code that was incompatible with other DNS implementations.

46:and specify the key's algorithm and secret on the command line. If the secret is longer than the digest length of the algorithm (64 bytes for SHA1 through SHA256, or 128 bytes for SHA384 and SHA512), then a new secret will be generated consisting of a hash digest of the old secret. (If the secret did not require conversion, then it will be printed without modification.)
/* Size of an SSL signature: MD5+SHA1 */
if (type == NID_md5_sha1)
if (type != NID_md5_sha1)
if ((type != NID_md5_sha1) && (s != NULL))
if (type == NID_md5_sha1)
if (type != NID_md5_sha1)
if ((type != NID_md5_sha1) && (s != NULL))

Event: diff -u /dev/null openssl/crypto/engine/hw_pk11so_pub.c:1.8.2.2
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:

/* Size of an SSL signature: MD5+SHA1 */
if (type == NID_md5_sha1)
if (type != NID_md5_sha1)
if ((type != NID_md5_sha1) && (s != NULL))

Event: BIND sources comment
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14538:+/* CKM_MD2_RSA_PKCS, CKM_MD5_RSA_PKCS, and CKM_SHA1_RSA_PKCS

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14542:+#define CKM_SHA1_RSA_PKCS 0x00000006

Event: BIND sources comment
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14550:+/* CKM_RSA_X9_31_KEY_PAIR_GEN, CKM_RSA_X9_31, CKM_SHA1_RSA_X9_31,

Event: BIND sources comment
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14551:+ * CKM_RSA_PKCS_PSS, and CKM_SHA1_RSA_PKCS_PSS are new for v2.11 */

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14554:+#define CKM_SHA1_RSA_X9_31 0x0000000C

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14556:+#define CKM_SHA1_RSA_PKCS_PSS 0x0000000E

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14560:+#define CKM_DSA_SHA1 0x00000012

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14746:+#define CKM_SSL3_SHA1_MAC 0x00000381

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14749:+#define CKM_SHA1_KEY_DERIVATION 0x00000032

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14765:+#define CKM_PBE_SHA1_CAST5_CBC 0x000003A5

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14766:+#define CKM_PBE_SHA1_CAST128_CBC 0x000003A5

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14767:+#define CKM_PBE_SHA1_RC4_128 0x000003A6

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14768:+#define CKM_PBE_SHA1_RC4_40 0x000003A7

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.0o-patch:14769:+#define CKM_PBE_SHA1_DES3_EDE_CBC 0x000003A8

Copyright ©2019, Infoblox, Inc. All right reserved.
Copyright ©2019, Infoblox, Inc. All right reserved.
11414:+ if ((type != NID_md5_sha1) && (s != NULL))

Event: BIND sources comment
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14433:+/* CKM_MD2_RSA_PKCS, CKM_MD5_RSA_PKCS, and CKM_SHA1_RSA_PKCS

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14437:+#define CKM_SHA1_RSA_PKCS 0x00000006

Event: BIND sources comment
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14445:+/* CKM_RSA_X9_31_KEY_PAIR_GEN, CKM_RSA_X9_31, CKM_SHA1_RSA_X9_31,

Event: BIND sources comment
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14446:+ * CKM_RSA_PKCS_PSS, and CKM_SHA1_RSA_PKCS_PSS are new for v2.11 */

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14449:+#define CKM_SHA1_RSA_X9_31 0x0000000C

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14451:+#define CKM_SHA1_RSA_PKCS_PSS 0x0000000E

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14455:+#define CKM_DSA_SHA1 0x00000012

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14641:+#define CKM_SSL3_SHA1_MAC 0x00000381

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14644:+#define CKM_SHA1_KEY_DERIVATION 0x00000392

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14660:+#define CKM_PBE_SHA1_CAST5_CBC 0x000003A5

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14661:+#define CKM_PBE_SHA1_CAST128_CBC 0x000003A5

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14662:+#define CKM_PBE_SHA1_RC4_128 0x000003A6

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14663:+#define CKM_PBE_SHA1_RC4_40 0x000003A7

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14664:+#define CKM_PBE_SHA1_DES3_EDE_CBC 0x000003A8

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14665:+#define CKM_PBE_SHA1_DES2_EDE_CBC 0x000003A9

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14666:+#define CKM_PBE_SHA1_RC2_128_CBC 0x000003AA

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14667:+#define CKM_PBE_SHA1_RC2_40_CBC 0x000003AB

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14672:+#define CKM_PBA_SHA1_WITH_SHA1_HMAC 0x000003C0
Event: BIND sources macro definition
Message: /fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:14743:+#define CKM_ECDSA_SHA1 0x00001042

Event: BIND sources macro definition
Message: /fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:15082:+#define CKG_MGF1_SHA1 0x00000001

Event: BIND sources macro definition
Message: /fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:15129:+#define CKD_SHA1_KDF 0x00000002

Event: BIND sources macro definition
Message: /fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:15186:+#define CKD_SHA1_KDF_ASN1 0x00000003

Event: BIND sources macro definition
Message: /fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:15187:+#define CKD_SHA1_KDF_CONCATENATE 0x00000004

Event: BIND sources macro definition
Message: /fipscc_nios/bind9/bin/pkcs11/openssl-1.0.1j-patch:15561:+#define CKP_PKCS5_PBKD2_HMAC_SHA1 0x00000001

Event: BIND sources comment
Message: /fipscc_nios/bind9/bin/pkcs11/pkcs11-keygen.8:50:can be specified as a DNSSEC signing algorithm that will be used with this key; for example, NSEC3RSASHA1 maps to RSA, and ECDSAP256SHA256 maps to ECC. The default class is "RSA".

Event: BIND sources comment
Message: /fipscc_nios/bind9/bin/pkcs11/pkcs11-keygen.c:231: * NSEC3RSASHA1 maps to RSA.

Event: diff -u /dev/null openssl/README.pkcs11:1.6.4.2
Message: /fipscc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:220:+ AES-256-ECB, AES-128-CTR, AES-192-CTR, AES-256-CTR, MD5, SHA1, SHA224,

Event: diff -u /dev/null openssl/crypto/engine/hw_pk11.c:1.26.4.4
Message: /fipscc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:

1146:+ PK11_SHA1,
1235:+ {PK11_SHA1, NID_sha1, CKM_SHA_1, },
1505:+ static const EVP_MD pk11_sha1 =
1507:+ NID_sha1,
1508:+ NID_sha1WithRSAEncryption,
3710:+ case NID_sha1:
3711:+ *digest = &pk11_sha1;

Event: diff -u /dev/null openssl/crypto/engine/hw_pk11so_pub.c:1.32.4.7
Message: /fipscc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:

6127:+/* Size of an SSL signature: MD5+SHA1 */
6689:+ if (type == NID_md5_sha1)
6734:+ if (type != NID_md5_sha1)
6783:+ if ((type != NID_md5_sha1) && (s != NULL))
6818:+ if (type == NID_md5_sha1)
6861:+ if (type != NID_md5_sha1)
6908:+ if ((type != NID_md5_sha1) && (s != NULL))

Event: diff -u /dev/null openssl/crypto/engine/hw_pk11so_pub.c:1.32.4.7
Message: /fipscc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:

11414:+/* Size of an SSL signature: MD5+SHA1 */
11444:+ if (type == NID_md5_sha1)
11489:+ if (type != NID_md5_sha1)
11538:+ if ((type != NID_md5_sha1) && (s != NULL))

Event: BIND sources comment
Message: /fipscc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14557:+/* CKM_MD2_RSA_PKCS, CKM_MD5_RSA_PKCS, and
CKM_SHA1_RSA_PKCS

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14561:+#define CKM_SHA1_RSA_PKCS 0x00000006

Event: BIND sources comment
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14569:+/* CKM_RSA_X9_31_KEY_PAIR_GEN, CKM_RSA_X9_31,
CKM_SHA1_RSA_X9_31,

Event: BIND sources: a literal in comments in the patch file openssl-0.9.8zc-patch
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14570:+ * CKM_RSA_PKCS_PSS, and CKM_SHA1_RSA_PKCS_PSS are new
for v2.11 */

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14573:+#define CKM_SHA1_RSA_X9_31 0x0000000C

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14579:+/* CKM_RSA_PKCS_PSS, and CKM_SHA1_RSA_PKCS_PSS are new
for v2.11 */

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14589:+#define CKM_PBE_SHA1_DES2_EDE_CBC 0x000003A9

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14590:+#define CKM_PBE_SHA1_RC2_128_CBC 0x000003AA

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14591:+#define CKM_PBE_SHA1_RC2_40_CBC 0x000003AB

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14596:+#define CKM_PBA_SHA1_WITH_SHA1_HMAC 0x000003C0

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14626:+#define CKM_ECDSA_SHA1 0x00001042

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14679:+#define CKM_PBE_SHA1_DES2_EDE_CBC 0x000003A9

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14686:+#define CKM_PBE_SHA1_RC2_128_CBC 0x000003AA

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14687:+#define CKM_PBE_SHA1_RC2_40_CBC 0x000003AB

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14756:+#define CKM_PBA_SHA1_WITH_SHA1_HMAC 0x000003C0

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14796:+#define CKM_PBA_SHA1_WITH_SHA1_HMAC 0x000003C0

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:14867:+#define CKM_ECDSA_SHA1 0x00001042

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:15206:+#define CKG_MGF1_SHA1 0x0000001

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:15253:+#define CKD_SHA1_KDF 0x00000002

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:15310:+#define CKD_SHA1_KDF ASN1 0x00000003

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:15311:+#define CKD_SHA1_KDF CONCATENATE 0x00000004

Event: BIND sources macro definition
Message: ./fipsc_nios/bind9/bin/pkcs11/openssl-0.9.8zc-patch:15685:+#define CKP_PKCS5_PBKD2_HMAC_SHA1 0x00000001

Event: BIND documentation
Message: ./fipsc_nios/bind9/bin/pkcs11/pkcs11-keygen.docbook:81: example, NSEC3RSASHA1 maps to RSA, and ECDSAP256SHA256 maps

Event: Code in function check_dnssec
Message: ./fipsc_nios/bind9/bin/named/update.c:2284: if (alg == DST_ALG_RSAMD5 || alg == DST_ALG_RSASHA1 ||

Event: Code in function dstkey_fromconfig
Message: ./fipsc_nios/bind9/bin/named/server.c:795: if ((keystruct.algorithm == DST_ALG_RSASHA1 ||

Event: Code in function load_configuration
Message: ./fipsc_nios/bind9/bin/named/server.c:
Event: Code in function compute_sit
Message: /fipscc_nios/bind9/bin/named/client.c:

```c
2460: #ifdef HMAC_SHA1_SIT
2461: unsigned char digest[ISC_SHA1_DIGESTLENGTH];
2464: isc_hmacsha1_t hmacsha1;
2471: isc_hmacsha1_init(&hmacsha1,
2473: ISC_SHA1_DIGESTLENGTH);
2474: isc_hmacsha1_update(&hmacsha1, cp, 16);
2478: isc_hmacsha1_update(&hmacsha1, client->cookie, sizeof(client->cookie));
2482: isc_hmacsha1_update(&hmacsha1);
2486: isc_hmacsha1_sign(&hmacsha1, digest, sizeof(digest));
2487: isc_hmacsha1_invalidate(&hmacsha1);
```

Event: Items of enum hmac inside struct keyalgorithms
Message: /fipscc_nios/bind9/bin/named/config.c:1148: enum { hmacnone, hmacmd5, hmacsha1, hmacsha24, ...

Event: Item of array algorithms of structs keyalgorithms
Message: /fipscc_nios/bind9/bin/named/config.c:1156: { "hmac-sha1", hmacsha1, DST_ALG_HMACSHA1, 160 }, ...

Event: Case of switch (algorithms[i].hmac) in function ns_config_getkeyalgorithm2
Message: /fipscc_nios/bind9/bin/named/config.c:1231: case hmacsha1: *name = dns_tsig_hmacsha1_name; break;

Event: BIND documentation
Message: /fipscc_nios/bind9/bin/nsupdate/nsupdate.docbook:166: hmac-sha1, hmac-sha224, ...

Event: BIND manual for nsupdate (i.e. man 1 nsupdate)
Message: /fipscc_nios/bind9/bin/nsupdate/nsupdate.1:104:hmac-sha1, ...

Event: Code in function parse_hmac
Message: /fipscc_nios/bind9/bin/nsupdate/nsupdate.c:

```c
477: } else if (strcasecmp(buf, "hmac-sha1") == 0) {
478: *hmac = DNS_TSIG_HMACSHA1_NAME;
479: } else if (strncasecmp(buf, "hmac-sha1-", 10) == 0) {
480: *hmac = DNS_TSIG_HMACSHA1_NAME;
```

Event: Case of switch (dst_key_alg(dstkey)) in function setup_keyfile
Message: /fipscc_nios/bind9/bin/nsupdate/nsupdate.c:

```c
702: case DST_ALG_HMACSHA1:
703: hmacname = DNS_TSIG_HMACSHA1_NAME;
```

Event: BIND manual for rndc (i.e. man 8 rndc)
Message: /fipscc_nios/bind9/bin/rndc/rndc.docbook:85: (for compatibility), HMAC-SHA1, HMAC-SHA224, HMAC-SHA256 (default), HMAC-SHA384 and HMAC-SHA512. They use a shared secret on each end of the connection. This provides TSIG-style authentication for the command request and the name server’s response. All commands sent over the channel must be signed by a key_id known to the server.

Event: Code in function parse_config
Message: /fipscc_nios/bind9/bin/rndc/rndc.c:

```c
609: else if (strcasecmp(algorithmstr, "hmac-sha1") == 0) {
610: algorithm = ISCCC_ALG_HMACSHA1;
```

Event: BIND documentation
Message: /fipscc_nios/bind9/bin/rndc/rndc.docbook:85: (for compatibility), HMAC-SHA1, HMAC-SHA224, HMAC-SHA256
Event: BIND documentation
Message: ./fipscc_nios/bind9/bin/mdc/docbook:718: is 1, representing SHA-1.

Event: BIND documentation
Message: ./fipscc_nios/bind9/bin/mdc/docbook:733: the SHA-1 hash algorithm, no opt-out flag,

Event: BIND documentation
Message: ./fipscc_nios/bind9/bin/mdc/docbook:125: (for compatibility), HMAC-SHA1, HMAC-SHA224, HMAC-SHA256

Event: BIND manual for mdc.conf (i.e. man 5 mdc.conf)
Message: ./fipscc_nios/bind9/bin/mdc/docbook.conf:103:to use; currently only HMAC-MD5 (for compatibility), HMAC-SHA1, HMAC-SHA224, HMAC-SHA256 (default), HMAC-SHA384 and HMAC-SHA512 are supported. This is followed by a secret clause which contains the base-64 encoding of the algorithm’s authentication key. The base-64 string is enclosed in double quotes.

Event: BIND sources, variable (Python dict) with hash algorithms gets initialized

Event: BIND sources, variable (Python dict) with hash algorithms gets initialized

Event: BIND sources, variable (Python tuple) with mnemonic names for algorithms gets initialized
Message: ./fipscc_nios/bind9/bin/python/dnssec-coverage.py.in:437: names = (None, 'RSAMDS', 'DH', 'DSA', 'ECC', 'RSASHA1', 'NSEC3DSA', 'NSEC3RSASHA1', 'RSASHA256', None)

Event: BIND manual for dnssec-dsfromkey (i.e. man 8 dnssec-dsfromkey)
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-dsfromkey.8:60:must be one of SHA-1 (SHA1), SHA-256 (SHA256), GOST or SHA-384 (SHA384). These values are case insensitive.

Event: Argument in call dns_ds_buildrdata in function loadds
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-signzone.c:1093: result = dns_ds_buildrdata(name, &key, DNS_DSDIGEST_SHA1,

Event: Code in function addnsec3param
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-signzone.c:2033: nsec3param.hash = unknownalg ? DNS_NSEC3_UNKNOWNALG : dns_hash_sha1;

Event: Code in function addnsec3
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-signzone.c:

2099: name, gorigin, dns_hash_sha1, iterations,
2105: DNS_NSEC3_UNKNOWNALG : dns_hash_sha1,
2108: nexthash, ISC_SHA1_DIGESTLENGTH,

Event: Argument in call dns_nsec3_hashname in function set_nsec3params
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-signzone.c:3156: gorigin, gorigin, dns_hash_sha1,

Event: Argument in call dns_nsec3_hashlength in function main
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-signzone.c:3298: DNS_DSDIGEST_SHA1,
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-signzone.c:4463: hash_length = dns_nsec3_hashlength(dns_hash_sha1);

Event: Argument in call nsec3ify in function main
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-signzone.c:4531: nsec3ify(dns_hash_sha1, nsec3iter, gsalt, salt_length,

Event: BIND documentation
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-dsfromkey.docbook:98: Use SHA-1 as the digest algorithm

Event: BIND documentation

Event: BIND documentation
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-dsfromkey.docbook:118: must be one of SHA-1 (SHA1),

Event: BIND documentation
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-keygen.docbook:120: of must be one of RSAMD5, RSASHA1,

Event: BIND documentation
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-keygen.docbook:121: DSA, NSEC3RSASHA1, NSEC3DSA, RSASHA256, RSASHA512, ECCGOST,

Event: BIND documentation
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-keygen.docbook:124: be DH (Diffie Hellman), HMAC-MD5, HMAC-SHA1, HMAC-SHA24,

Event: BIND documentation
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-keygen.docbook:129: If no algorithm is specified, then RSASHA1 will be used

Event: BIND documentation
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-keygen.docbook:131: in which case NSEC3RSASHA1 will be used instead.

Event: BIND documentation
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-keygen.docbook:136: Note 1: that for DNSSEC, RSASHA1 is a mandatory to implement

Event: BIND documentation
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-keygen.docbook:141: Note 2: DH, HMAC-MD5, and HMAC-SHA1 through HMAC-SHA512

Event: BIND documentation
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-keygen.docbook:192: set on the command line, NSEC3RSASHA1 will be used

Event: BIND sources macro definition
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-keyfromlabel.c:55:#define DEFAULT_ALGORITHM "RSASHA1"

Event: BIND sources macro definition
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-keyfromlabel.c:56:#define DEFAULT_NSEC3_ALGORITHM "NSEC3RSASHA1"

Event: algs - algorithms string
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-keyfromlabel.c:

58: static const char *algs = "RSA | RSAMD5 | DH | DSA | RSASHA1 |"
59: " NSEC3DSA | NSEC3RSASHA1 |"

Event: Code of function usage
Message: /fipscc_nios/bind9/bin/dnssec/dnssec-keyfromlabel.c:

77: fprintf(stderr, " (default: RSASHA1, or "
78: "NSEC3RSASHA1 if using -3)\n");
Event: Code in function main
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-keyfromlabel.c:400: alg != DST_ALG_NSEC3DSA & alg != DST_ALG_NSEC3RSASHA1 &

Event: BIND manual for dnssec-keygen (i.e. man 8 dnssec-keygen)
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-keygen.8:
51: must be one of RSAMD5, RSASHA1, DSA, NSEC3RSASHA1, NSEC3DSA, RSASHA256, RSASHA512, ECCGOST, ECDSAP256SHA256 or ECDSAP384SHA384. For TSIG/TKEY, the value must be DH (Diffie Hellman), HMAC\-MD5, HMAC\-SHA1, HMAC\-SHA224, HMAC\-SHA256, HMAC\-SHA384, or HMAC\-SHA512. These values are case insensitive.
53: If no algorithm is specified, then RSASHA1 will be used by default, unless the
55: option is specified, in which case NSEC3RSASHA1 will be used instead. (If
59: Note 1: that for DNSSEC, RSASHA1 is a mandatory to implement algorithm, and DSA is recommended. For TSIG, HMAC\-MD5
is mandatory.
61: Note 2: DH, HMAC\-MD5, and HMAC\-SHA1 through HMAC\-SHA512 automatically set the \-T KEY option.
84: Use an NSEC3\-capable algorithm to generate a DNSSEC key. If this option is used and no algorithm is explicitly set on the
command line, NSEC3RSASHA1 will be used by default. Note that RSASHA256, RSASHA512, ECCGOST, ECDSAP256SHA256
and ECDSAP384SHA384 algorithms are NSEC3\-capable.

Event: BIND manual for dnssec-keyfromlabel (i.e. man 8 dnssec-keyfromlabel)
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-keyfromlabel.8:
51: must be one of RSAMD5, RSASHA1, DSA, NSEC3RSASHA1, NSEC3DSA, RSASHA256, RSASHA512, ECCGOST, ECDSAP256SHA256 or ECDSAP384SHA384. These values are case insensitive.
53: If no algorithm is specified, then RSASHA1 will be used by default, unless the
55: option is specified, in which case NSEC3RSASHA1 will be used instead. (If
59: Note 1: that for DNSSEC, RSASHA1 is a mandatory to implement algorithm, and DSA is recommended. For TSIG, HMAC\-MD5
is mandatory.
61: Note 2: DH, HMAC\-MD5, and HMAC\-SHA1 through HMAC\-SHA512 automatically set the \-T KEY option.
84: Use an NSEC3\-capable algorithm to generate a DNSSEC key. If this option is used and no algorithm is explicitly set on the
command line, NSEC3RSASHA1 will be used by default.

Event: BIND documentation
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-keyfromlabel.docbook:104: must be one of RSAMD5, RSASHA1,

Event: BIND documentation
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-keyfromlabel.docbook:105: DSA, NSEC3RSASHA1, NSEC3DSA, RSASHA256, RSASHA512, ECCGOST,

Event: BIND documentation
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-keyfromlabel.docbook:110: If no algorithm is specified, then RSASHA1 will be used

Event: BIND documentation
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-keyfromlabel.docbook:112: in which case NSEC3RSASHA1 will be used instead.

Event: BIND documentation
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-keyfromlabel.docbook:117: Note 1: that for DNSSEC, RSASHA1 is a mandatory to implement

Event: BIND documentation
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-keyfromlabel.docbook:132: set on the command line, NSEC3RSASHA1 will be used

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-keygen.c:82:#define DEFAULT_ALGORITHM "RSASHA1"

Event: BIND sources macro definition
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-keygen.c:83:#define DEFAULT_NSEC3_ALGORITHM "NSEC3RSASHA1"

Event: BIND sources string literal
Message: ./fipscc_nios/bind9/bin/dnssec/dnssec-keygen.c:99: fprintf(stderr, " RSA | RSAMD5 | DSA | RSASHA1 | NSEC3RSASHA1"
Event: BIND sources string literal
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-keygen.c:103: fprintf(stderr, " DH | HMAC-MD5 | HMAC-SHA1 | HMAC-SHA224 | *

Event: BIND sources string literal
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-keygen.c:106: fprintf(stderr, " (default: RSASHA1, or *

Event: BIND sources string literal
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-keygen.c:107: "NSEC3RSASHA1 if using -3")

Event: BIND sources string literal
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-keygen.c:111: fprintf(stderr, " RSASHA1: [512..%d]n", MAX_RSA);

Event: BIND sources string literal
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-keygen.c:112: fprintf(stderr, " NSEC3RSASHA1: [512..%d]n", MAX_RSA);

Event: BIND sources string literal
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-keygen.c:123: fprintf(stderr, " HMAC-SHA1: [1..160]n");

Event: Code in function main
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-keygen.c:

564: alg = DST_ALG_HMACSHA1;
587: alg != DST_ALG_NSEC3DSA && alg != DST_ALG_NSEC3RSASHA1 &&

Event: Cases of switch (alg) in function main
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-keygen.c:

733: case DNS_KEYALG_RSASHA1:
734: case DNS_KEYALG_NSEC3RSASHA1:
771: case DST_ALG_HMACSHA1:
774: fatal("HMAC-SHA1 key size %d out of range", size);
776: fatal("HMAC-SHA1 digest bits %d out of range", dbits);
778: fatal("HMAC-SHA1 digest bits %d not divisible by 8");

Event: Code in function main
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-keygen.c:670: alg == DST_ALG_HMACSHA1 || alg == DST_ALG_HMACSHA224 ||

Event: Cases of switch (alg) in function main
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-keygen.c:

878: case DNS_KEYALG_RSASHA1:
879: case DNS_KEYALG_NSEC3RSASHA1:
898: case DST_ALG_HMACSHA1:

Event: Code in function usage
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-dsfromkey.c:

336: "(SHA-1, SHA-256, GOST or SHA-384)n";
337: fprintf(stderr, " -1: use SHA-1n");

Event: Initializing local variable dtype in function main
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-dsfromkey.c:358: unsigned int dtype = DNS_DSDIGEST_SHA1;

Event: Setting variable dtype in function main
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-dsfromkey.c:388: dtype = DNS_DSDIGEST_SHA1;

Event: Code in function main
Message: /lipsc_nios/bind9/bin/dnssec/dnssec-dsfromkey.c:
458: if (strcasecmp(algname, "SHA1") == 0 ||
459: strcasecmp(algname, "SHA-1") == 0)
460: dtype = DNS_DSDIGEST_SHA1;
535: emit(DNS_DSDIGEST_SHA1, showall, lookaside,
549: emit(DNS_DSDIGEST_SHA1, showall, lookaside, &rdata);

Event: Calculate fingerprint of VMWare config and disk of the product image
Message: /fipscc_nios/vnios/vnios-build:707: openssl sha1 ${input_file}*.ovf ${name}*.vmdk > ${input_file}.mf

Event: Calculate fingerprint of VMWare config and disk of the product image

Event: Comment in NIOS build scripts
Message: /fipscc_nios/vnios/vnios-build:1221: # Generates an mf file. Pretty simple, just dumps the SHA1 fingerprints

Event: Calculate fingerprint of VMWare config and disk of the product image
Message: /fipscc_nios/vnios/vnios-build:1236: openssl sha1 ${name}*.ovf,vmdk > ${output}.mf

Event: OpenSSL binary library
Message: Binary file ./fipscc_nios/vnios/libdir/lib/libcrypto.so.0.9.8/libcrypto.so.0.9.8 matches

Event: OpenSSL binary library
Message: Binary file ./fipscc_nios/vnios/libdir/lib/libssl.so.0.9.8/libssl.so.0.9.8 matches

Event: Comment in .ova packaging script

Event: Calculate fingerprint of VMWare .ova file of the product image
Message: /fipscc_nios/vnios/build-ova.sh:66: openssl sha1 "${baseFile}" >${mfFile}

Event: Calculate fingerprint of VMWare .ova file of the product image
Message: /fipscc_nios/vnios/build-ova.sh:73: openssl sha1 "${baseFile}" >>${mfFile}

Event: Check algorithm name and set algorithm code in function isclib_make_dst_key
Message: /fipscc_nios/dhcp3/omapip/isclib.c:
344: } else if (strcasecmp(algorithm, DHCP_HMAC_SHA1_NAME) == 0) {
345: algorithm_code = DST_ALG_HMACSHA1;

Event: ISC DHCP macro define
Message: /fipscc_nios/dhcp3/includes/isc-dhcp/dst.h:117: #define KEY_HMAC_SHA1 158

Event: ISC DHCP macro define
Message: /fipscc_nios/dhcp3/includes/isc-dhcp/dst.h:119: #define DST_MAX_ALGS KEY_HMAC_SHA1

Event: ISC DHCP macro define
Message: /fipscc_nios/dhcp3/includes/omapip/isclib.h:109: #define DHCP_HMAC_SHA1_NAME "HMAC-SHA1.SIG-ALG.REG.INT."

Event: ISC DHCP config sample
Message: /fipscc_nios/dhcp3/server/dhcpd.conf.5:1321: HMAC-SHA1

Event: ISC DHCP documentation
Message: /fipscc_nios/dhcp3/RELNOTES:271: additional algorithms: hmac-sha1, hmac-sha224, hmac-sha256, hmac-sha384,

Event: OpenSSL binary library
Message: Binary file ./fipscc_nios/ipamvm/libcrypto.so.0.9.8 matches

Event: OpenSSL binary library
Message: Binary file ./fipscc_nios/ipamvm/libssl.so.0.9.8 matches

Event: Argument of call MemBufferWriteString in function LogTlsLogExtended
Message: ./fipscc_nios/sw_atp/suricata/src/log-tlslog.c:89: MemBufferWriteString(aft->buffer, " SHA1='%s'", stateserver_connp.cert0_fingerprint);

Event: Assigning field desc of sigmatch_table in function DetectTlsRegister

Event: Call of ComputeSHA1 in function DecodeTLSHandshakeServerCertificate
Message: ./fipscc_nios/sw_atp/suricata/src/app-layer-tls-handshake.c:172: hash = ComputeSHA1((unsigned char *) input, (int) msg_len);
Message: ./fipscc_nios/sw_atp/suricata/src/app-layer-tls-handshake.c:172: hash = ComputeSHA1((unsigned char *) input, (int) msg_len);

Event: Assigning field desc of sigmatch_table in function DetectTlsRegister

Event: Copy state in function Sha1Compress
Message: ./fipscc_nios/sw_atp/suricata/src/util-crypt.c:44:static int Sha1Compress(HashState *md, unsigned char *buf);
Message: ./fipscc_nios/sw_atp/suricata/src/util-crypt.c:44:static int Sha1Compress(HashState *md, unsigned char *buf);

Event: Store state in function Sha1Compress
Message: ./fipscc_nios/sw_atp/suricata/src/util-crypt.c:44:static int Sha1Compress(HashState *md, unsigned char *buf);
Message: ./fipscc_nios/sw_atp/suricata/src/util-crypt.c:44:static int Sha1Compress(HashState *md, unsigned char *buf);

Event: Function Sha1Compress definition
Message: ./fipscc_nios/sw_atp/suricata/src/app-layer-tls-handshake.c:172: hash = ComputeSHA1((unsigned char *) input, (int) msg_len);
Message: ./fipscc_nios/sw_atp/suricata/src/app-layer-tls-handshake.c:172: hash = ComputeSHA1((unsigned char *) input, (int) msg_len);

Event: Function Sha1Compress definition
Message: ./fipscc_nios/sw_atp/suricata/src/util-crypt.c:44:static int Sha1Compress(HashState *md, unsigned char *buf);
Message: ./fipscc_nios/sw_atp/suricata/src/util-crypt.c:44:static int Sha1Compress(HashState *md, unsigned char *buf);

Event: State initialization in function Sha1Init
Message: ./fipscc_nios/sw_atp/suricata/src/util-crypt.c:121:static int Sha1Init(HashState * md)
Message: ./fipscc_nios/sw_atp/suricata/src/util-crypt.c:121:static int Sha1Init(HashState * md)

Event: Function Sha1Compress definition
Message: ./fipscc_nios/sw_atp/suricata/src/util-crypt.c:121:static int Sha1Init(HashState * md)
Message: ./fipscc_nios/sw_atp/suricata/src/util-crypt.c:121:static int Sha1Init(HashState * md)

Event: Code in function Sha1Compress
Message: ./fipscc_nios/sw_atp/suricata/src/util-crypt.c:
146: if (md->sha1.curlen > sizeof(md->sha1.buf)) {
150: if (md->sha1.curlen == 0 & inlen >= 64) {
151: if ((err = Sha1Compress(md, (unsigned char *)in)) != SC_SHA_1_OK) {
154: md->sha1.length += 64 * 8;
158: n = MIN(inlen, (64 - md->sha1.curlen));
160: md->sha1.curlen += n;
163: if (md->sha1.curlen == 64) {
164: if ((err = Sha1Compress(md, md->sha1.buf)) != SC_SHA_1_OK) {
167: md->sha1.length += 8*64;
168: md->sha1.curlen = 0;

Event: Function Sha1Done definition
Message: /fipscc_nios/sw_atp/suricata/src/util-crypt.c:177:static int Sha1Done(HashState * md, unsigned char *out)

Event: Code in function Sha1Done
Message: /fipscc_nios/sw_atp/suricata/src/util-crypt.c:

186: if (md->sha1.curlen >= sizeof(md->sha1.buf)) {
191: md->sha1.length += md->sha1.curlen * 8;
194: md->sha1.buf[md->sha1.curlen++] = (unsigned char)0x80;
200: if (md->sha1.curlen > 56) {
201: while (md->sha1.curlen < 64) {
202: md->sha1.buf[md->sha1.curlen++] = (unsigned char)0;
204: Sha1Compress(md, md->sha1.buf);
205: md->sha1.curlen = 0;
209: while (md->sha1.curlen < 56) {
210: md->sha1.buf[md->sha1.curlen++] = (unsigned char)0;
214: STORE64H(md->sha1.length, md->sha1.buf+56);
215: Sha1Compress(md, md->sha1.buf);
219: STORE32H(md->sha1.state[i], out+(4*i));

Event: ComputeSHA1 definition
Message: /fipscc_nios/sw_atp/suricata/src/util-crypt.c:227:unsigned char* ComputeSHA1(unsigned char* buff, int bufflen)

Event: Code in function ComputeSHA1
Message: /fipscc_nios/sw_atp/suricata/src/util-crypt.c:

233: Sha1Init(&md);
234: Sha1Process(&md, buff, bufflen);
235: Sha1Done(&md, IResultado);

Event: Function ComputeSHA1 definition if HAVE_NSS is defined
Message: /fipscc_nios/sw_atp/suricata/src/util-crypt.c:241:unsigned char* ComputeSHA1(unsigned char* buff, int bufflen)

Event: Code in function ComputeSHA1
Message: /fipscc_nios/sw_atp/suricata/src/util-crypt.c:

243: HASHContext *sha1_ctx = HASH_Create(HASH_AlgSHA1);
246: if (sha1_ctx == NULL) {
252: HASH_Destroy(sha1_ctx);
256: HASH_Begin(sha1_ctx);
257: HASH_Update(sha1_ctx, buff, bufflen);
258: HASH_Destroy(sha1_ctx);

Event: Code in function process
Message: /fipscc_nios/sw_atp/suricata/contrib/file_processor/Processor/ShadowServer.pm:32: my @meta_cols = qw(md5 sha1 first_date last_date type ssdeep);

Event: atp rule

Copyright ©2019, Infoblox, Inc. All right reserved.
Event: sid-msg.map items
Message: /fipscc_nios/sw_atp/suricata/prod_suricata/suricata/rules.orig/sid-msg.map:
14240:2017120 || ET POLICY Possible IPMI 2.0 RAKP Remote SHA1 Password Hash Retrieval RAKP message 1 with default BMC usernames (Admin|root|Administrator|USERID)
14241:2017121 || ET ATTACK_RESPONSE Possible IPMI 2.0 RAKP Remote SHA1 Password Hash Retrieval RAKP message 2 status code Unauthorized Name

Event: atp rule
Message: /fipscc_nios/sw_atp/suricata/prod_suricata/suricata/rules.orig/emerging-policy.rules:2342:alert udp $EXTERNAL_NET any -> $HOME_NET 623 (msg:"ET POLICY Possible IPMI 2.0 RAKP Remote SHA1 Password Hash Retrieval RAKP message 1 with default BMC usernames (Admin|root|Administrator|USERID)"; content:"|06 12|"; offset:4; depth:2; pcre:"/((\x0d|\x05)Admin(istrator)?|\x04root|\x06USERID)/Ri"; classtype:protocol-command-decode; sid:2017120; rev:2;)

Event: atp rule
Message: /fipscc_nios/sw_atp/suricata/prod_suricata/suricata/rules.orig/emerging-attack_response.rules:481:alert udp $HOME_NET 623 -> $EXTERNAL_NET any (msg:"ET ATTACK_RESPONSE Possible IPMI 2.0 RAKP Remote SHA1 Password Hash Retrieval RAKP message 2 status code Unauthorized Name"; content:"|06 13|"; offset:4; depth:2; content:"|0d|"; distance:11; within:1; classtype:protocol-command-decode; sid:2017121; rev:2;)

Event: Argument of call EVP_BytesToKey which makes 3DES key out of the password in function generateDESKey
Message: /fipscc_nios/common/server/src/lib/security/security_functions.c:64: EVP_sha1(),

Event: Code in function ib_bin_SHAHash - SHA hash function which returns the digest data in a buffer with length 20
Message: /fipscc_nios/common/server/src/lib/security/security_functions.c:

305: SHA1_Init(&c);
306: SHA1_Update(&c, inputValue, inputLength);
307: SHA1_Final(sha, &c);

Comment to function ib_ssha_pwd
Message: /fipscc_nios/common/server/include/infoblox/security_functions.h:298: * This routine implements the salted SHA1 for password hashing.

Comment to function ib_ssha_pwd
Message: /fipscc_nios/common/server/include/infoblox/security_functions.h:298: * This routine implements the salted SHA1 for password hashing.

Cases of switch ((sldns_algorithm)alg) in function sldns_rr_dnskey_key_size_raw
Message: /fipscc_nios/unbound/ldns/keyraw.c:

50: case LDNS_RSASHA1:
51: case LDNS_RSASHA1_NSEC3:

Items of sldns_lookup_table sldns_algorithms_data - lookup table for standard DNS stuff
Message: /fipscc_nios/unbound/ldns/wire2str.c:

42: { LDNS_RSASHA1, "RSASHA1" },
43: { LDNS_DSA_NSEC3, "DSA-NSEC3-SHA1" },
44: { LDNS_RSASHA1_NSEC3, "RSASHA1-NSEC3-SHA1" },

Item of sldns_lookup_table sldns_hashes_data - hash algorithms in DS record
Message: /fipscc_nios/unbound/ldns/wire2str.c:59: { LDNS_SHA1, "SHA1" },

Argument in call sldns_str_print in function sldns_wire2str_edns_n3u_print
Message: /fipscc_nios/unbound/ldns/wire2str.c:1766: w += sldns_str_print(s, sl, " SHA1");

Items of enum sldns_enum_algorithm - algorithms used in dns
Message: /fipscc_nios/unbound/ldns/rdef.h:

364: LDNS_RSASHA1 = 5,
366: LDNS_RSASHA1_NSEC3 = 7,
Event: Item of enum sldns_enum_hash - hashing algorithms used in the DS record
Message: ./fipscc_nios/unbound/ldns/rrdef.h:383: LDNS_SHA1 = 1, /* RFC 4034 */

Event: Content of autoconf file
Message: ./fipscc_nios/unbound/configure.ac:573:AC_CHECK_FUNCS([OPENSSL_config EVP_sha1 EVP_sha256 EVP_sha512 FIPS_mode])

Event: Case of switch(d->rr_data[i][2+0]) in function nsec3_known_algo which returns if nsec3 RR has known algorithm
Message: ./fipscc_nios/unbound/validator/val_nsec3.c:171: case NSEC3_HASH_SHA1:

Event: Code in case NSEC3_HASH_SHA1 of switch(algo) in function nsec3_get_hashed
Message: ./fipscc_nios/unbound/validator/val_nsec3.c:
549: #if defined(HAVE_EVP_SHA1) || defined(HAVE_NSS)
550: case NSEC3_HASH_SHA1:
554: hash_len = SHA1_LENGTH;
559: (void)SHA1((unsigned char*)sldns_buffer_begin(buf),
563: (void)HASH_HashBuf(HASH_AlgSHA1, (unsigned char*)res,
573: (void)SHA1
578: (void)HASH_HashBuf(HASH_AlgSHA1,

Event: Unbound sources comment
Message: ./fipscc_nios/unbound/validator/val_nsec3.c:585:#endif /* HAVE_EVP_SHA1 or NSS */

Event: Code in case NSEC3_HASH_SHA1 of switch(algo) in function nsec3_calc_hash which performs hash of name
Message: ./fipscc_nios/unbound/validator/val_nsec3.c:
611: #if defined(HAVE_EVP_SHA1) || defined(HAVE_NSS)
612: case NSEC3_HASH_SHA1:
616: c->hash_len = SHA1_LENGTH;
623: (void)SHA1((unsigned char*)sldns_buffer_begin(buf),
627: (void)HASH_HashBuf(HASH_AlgSHA1,
638: (void)SHA1
643: (void)HASH_HashBuf(HASH_AlgSHA1,

Event: Unbound sources comment
Message: ./fipscc_nios/unbound/validator/val_nsec3.c:650:#endif /* HAVE_EVP_SHA1 or NSS */

Event: Case of switch(algo) in function ds_digest_size_supported(int algo) which returns size of DS digest according to its hash algorithm
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:
82: #ifdef HAVE_EVP_SHA1
83: case LDNS_SHA1:

Event: Case of switch(algo) in function secalgo_ds_digest
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:
122: #ifdef HAVE_EVP_SHA1
123: case LDNS_SHA1:
124: (void)SHA1(buf, len, res);

Event: Cases of switch(id) in function dnskey_algo_id_is_supported which returns true if DNSKEY algorithm id is supported
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:
161: case LDNS_RSASHA1:
162: case LDNS_RSASHA1_NSEC3:

Event: Cases of switch(algo) in function setup_key_digest which setups key and digest for verification
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:
323: case LDNS_RSASHA1:
324: case LDNS_RSASHA1_NSEC3:

Event: Code in case LDNS_RSASHA512 of switch(algo) in function setup_key_digest
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:359: "digest_type = EVP_sha1();"

Event: Case of switch(algo) in function ds_digest_size_supported
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:
   572: case LDNS_SHA1;
   573: return SHA1_LENGTH;

Event: Case of switch(algo) in function secalgo_ds_digest
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:
   595: case LDNS_SHA1;
   596: return HASH_HashBuf(HASH_AlgSHA1, res, buf, len)

Event: Cases of switch(id) in function dnskey_algo_id_is_supported
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:
   627: case LDNS_RSASHA1;
   628: case LDNS_RSASHA1_NSEC3:

Event: Code in function SECKEYPublicKey* nss_buf2dsa(unsigned char* key, size_t len)
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:
   743: if(len < (size_t)1 + SHA1_LENGTH + 3*length)
   747: Q.len = SHA1_LENGTH;
   748: offset += SHA1_LENGTH;

Event: hash prefix to prepend to hash output, from RFC3110
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:
   853: static unsigned char p_sha1[] = {0x30, 0x21, 0x30, 0x09, 0x06, 0x05, 0x2B,

Event: Code in case LDNS_DSA, case LDNS_DSA_NSEC3 of switch(algo) in function nss_setup_key_digest
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:
   874: "htype = HASH_AlgSHA1;"

Event: Cases of switch(algo) in function nss_setup_key_digest
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:
   877: case LDNS_RSASHA1;
   878: case LDNS_RSASHA1_NSEC3:

Event: Code in case LDNS_RSASHA512 of switch(algo) in function nss_setup_key_digest which setups key and digest for verification
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:
   906: "htype = HASH_AlgSHA1;"
   907: "prefix = p_sha1;"
   908: "prefixlen = sizeof(p_sha1);"

Event: Code in function verify_canonrrset which checks a canonical sig+rrset and signature against a dnskey
Message: ./fipscc_nios/unbound/validator/val_secalgo.c:
   995: if(sigblock_len == 1+2*SHA1_LENGTH) {

Event: Unbound sources macro definition
Message: ./fipscc_nios/unbound/validator/val_nsec3.h:
   96:"/** The SHA1 hash algorithm for NSEC3 */
   97:#define NSEC3_HASH_SHA1 0x01

Event: Unbound sources macro undefined
Message: ./fipscc_nios/unbound/config.h.in:
   116:"/* Define to 1 if you have the 'EVP_sha1' function. */
   117:#undef HAVE_EVP_SHA1

Event: Argument of call verifytest_file in function verify_test
Message: ./fipscc_nios/unbound/testcode/unitverify.c:509: verifytest_file("testdata/test_sigs.sha1_and_256", "20070829144150");
Event: Argument of call dstest_file in function verify_test
Message:./fipscc_nios/unbound/testcode/unitverify.c:530: dstest_file("testdata/test_ds.sha1");

Event: Unbound documentation
Message:./fipscc_nios/unbound/doc/Changelog:2185: - change unbound-control-setup from 1024(sha1) to 1536(sha256).

Event: Unbound documentation
Message:./fipscc_nios/unbound/doc/Changelog:3396: - fixup SHA256 DS downgrade, no longer possible to downgrade to SHA1.

Event: Content of diff file for validator/val_secalgo.c
Message:./fipscc_nios/unbound/contrib/patch_rsamd5_enable.diff:
13: case LDNS_RSASHA1:
22: case LDNS_RSASHA1:

Event: Code in bash script configure
Message:./fipscc_nios/unbound/configure:16735:for ac_func in OPENSSL_config EVP_sha1 EVP_sha256 EVP_sha512 FIPS_mode

Event: Binary JAR file for our Web UI

Event: Encryption types
Message:./fipscc_nios/webui/platform/src/plugins/com.infoblox.util.localization/src/com/infoblox/util/localization/messages.properties:
3338:EncType.AES_128_CTS_HMAC_SHA_1_96=aes128-cts-hmac-sha1-96
3339:EncType.AES_256_CTS_HMAC_SHA_1_96=aes256-cts-hmac-sha1-96

Event: Algorithm key enumeration items
Message:./fipscc_nios/webui/platform/src/plugins/com.infoblox.util.localization/src/com/infoblox/util/localization/messages.properties:
3743:AlgorithmKeyEnum.SHA_1_1024=SHA-1 1024
3744:AlgorithmKeyEnum.SHA_1_2048=SHA-1 2048

Event: Pre-defined authentication types in BFD template
Message:./fipscc_nios/webui/platform/src/plugins/com.infoblox.util.localization/src/com/infoblox/util/localization/messages.properties:
4023:BFDTemplatesAuthType.SHA1 = SHA-1
4024:BFDTemplatesAuthType.METICULOUS-SHA1 = Meticulous SHA-1

Event: Algorithm types
Message:./fipscc_nios/webui/platform/src/plugins/com.infoblox.module.dns/src/com/infoblox/module/dns/localization/messages.properties:
47:AlgorithmType.RsaSha1.5=RSA/SHA1 (5)
48:AlgorithmType.RsaSha1Nsec3.7=RSA/SHA1/NSEC3 (7)

Event: Algorithm types
Message:./fipscc_nios/webui/platform/src/plugins/com.infoblox.module.dns/src/com/infoblox/module/dns/localization/messages.properties:
7:AlgorithmType.5=RSA/SHA-1
9:AlgorithmType.7=RSA/SHA-1(NSEC3)

Event: Algorithm types
Message:./fipscc_nios/webui/platform/src/plugins/com.infoblox.module.dns/src/com/infoblox/nios/ui/widget/editor/zone/auth/dnssec/AbstractSigningKeysTablePanel.properties:
8:AlgorithmType.RsaSha1.5=RSA/SHA1 (5)
9:AlgorithmType.RsaSha1Nsec3.7=RSA/SHA1/NSEC3 (7)

Event: Algorithm type
Message:./fipscc_nios/webui/platform/src/plugins/com.infoblox.module.dns/src/com/infoblox/nios/ui/widget/editor/common/panel/dnssec/DnsSecTablePanel.properties:
8:AlgorithmType.RsaSha1.5=RSA/SHA1 (5)
9:AlgorithmType.RsaSha1Nsec3.7=RSA/SHA1/NSEC3 (7)
Event: Python documentation

Event: Check algorithm type in function gen_hsm_client_cert
Message: ./fipscc_nios/products/one/script/Infoblox/Session.pm:1501: if ($args{'algorithm'} !~ /^(RSASHA1|RSASHA256)$/) {

Event: Error message in function gen_hsm_client_cert
Message: ./fipscc_nios/products/one/script/Infoblox/Session.pm:1502: set_error_codes(1103, $args{'algorithm'} . ' is an unsupported algorithm, valid values are: RSASHA1 or RSASHA256', $self);

Event: Check algorithm type in function export_data
Message: ./fipscc_nios/products/one/script/Infoblox/Session.pm:5950: if ($args{'algorithm'} !~ /^(RSASHA1|RSASHA256)$/) {

Event: Error message in function export_data
Message: ./fipscc_nios/products/one/script/Infoblox/Session.pm:5951: return set_error_codes(1103, $args{'algorithm'} . ' is an unsupported algorithm, valid values are: RSASHA1 or RSASHA256', $self);

Event: Algorithm type in _allowed_members
Message: ./fipscc_nios/products/one/script/Infoblox/IBAP/DNS_Zone.pm:4449: 'algorithm' => {simple => 'asis', enum => ['RSAMD5', 'DSA', 'RSASHA1', 'RSASHA256', 'RSASHA512']},

Event: Enum items in function enctype
Message: ./fipscc_nios/products/one/script/Infoblox/IBAP/Grid_Misc.pm:
469: 'aes128-cts-hmac-sha1-96',
470: 'aes256-cts-hmac-sha1-96',

Event: Authentication type in %_allowed_members
Message: ./fipscc_nios/products/one/script/Infoblox/IBAP/Grid_Misc.pm:1655: 'authentication_type' => {simple => 'asis', enum => ['NONE', 'MD5', 'METICULOUS-MD5', 'SHA1', 'METICULOUS-SHA1']},

Event: Digest type in _allowed_members
Message: ./fipscc_nios/products/one/script/Infoblox/IBAP/DNS_RecordsDNSSec.pm:350: 'digest_type' => {readonly => 1, enum => ['SHA1', 'SHA256', '1', '2']},

Event: Item of digest type mappings
Message: ./fipscc_nios/products/one/script/Infoblox/IBAP/DNS_RecordsDNSSec.pm:390: 'SHA1' => 'SHA_1',

Event: Item of reverse digest type mappings
Message: ./fipscc_nios/products/one/script/Infoblox/IBAP/DNS_RecordsDNSSec.pm:397: 'SHA_1' => 'SHA1',

Event: Items of _alg_hash_ mappings
Message: ./fipscc_nios/products/one/script/Infoblox/Util.pm:
7675: 5 => 'RSASHA1',
7677: 7 => 'NSEC3RSASHA1',

Event: Algorithm mappings for dnssec KSK and ZSK algorithms
Message: ./fipscc_nios/products/one/script/Infoblox/Util.pm:
7795: | RSASHA1 | RSASHA1 | NSEC |
7797: | NSEC3RSASHA1 | RSASHA1 | NSEC3 |
7804: | 5 | RSASHA1 | NSEC |
7808: | 7 | RSASHA1 | NSEC3 |

Event: Items of mappings _nsec3_algorithm_mappings
Message: ./fipscc_nios/products/one/script/Infoblox/Util.pm:
7816: NSEC3RSASHA1 => 'RSASHA1',
7818: 7 => 'RSASHA1',

Event: Items of mappings _nsec_algorithm_mappings
Message: ./fipscc_nios/products/one/script/Infoblox/Util.pm:
7827: RSASHA1 => 'RSASHA1',
7832: 5 => 'RSASHA1',

Event: Comments in function dnssec_key_algorithms_list_update
Message: /fipscc_nios/products/one/script/Infoblox/Util.pm:

7984: # dnssec_ksk_algorithm -> NSEC3RSASHA1, next_secure_type -> NSEC3
7985: # if we change dnssec_ksk_algorithm -> RSASHA1,

Event: Dictionary of possible authentication types in NIOS IBAP for BFD

Event: Constant definitions
Message: /fipscc_nios/products/one/server/src/lib/one_safenet/cryptoki.h:

391:#define CKA_FINGERPRINT_SHA1 (CKA_VENDOR_DEFINED | 0x0002):
423:#define CKM_SHA1_RSA_PKCS 0x00000006
427:#define CKM_SHA1_RSA_X9_31 0x0000000C
429:#define CKM_SHA1_RSA_PKCS_PSS 0x0000000E
433:#define DSA_SHA1 0x00000012
549:#define SSL3_SHA1 MAC 0x00000381
552:#define SHA1_KEY_DERIVATION 0x00000392
563:#define PBE_SHA1 CAST5_CBC 0x000003A5
563:#define PBE_SHA1 CAST5_CBC 0x000003A5
564:#define PBE_SHA1 CAST128_CBC 0x000003A5
565:#define PBE_SHA1 RC4_128 0x000003A6
566:#define PBE_SHA1 RC4_40 0x000003A7
567:#define PBE_SHA1 DES3_EDE_CBC 0x000003A8
568:#define PBE_SHA1 DES2_EDE_CBC 0x000003A9
569:#define PBE_SHA1 RC2_128_CBC 0x000003AA
570:#define PBE_SHA1 RC2_40_CBC 0x000003AB
606:#define ECDSA_SHA1 0x00010402
659:#define SHA1_KEY_DERIVATION_OLD XXX CKM_VENDOR_DEFINED_OLD XXX + 20 // SPKM & SLL added capabilities
665:#define PBE_SHA1 CAST5_CBC_OLD XXX CKM_VENDOR_DEFINED_OLD XXX + 26 // Entrust added capabilities
674:#define PBE_SHA1 DES3_EDE_CBC_OLD XXX CKM_VENDOR_DEFINED_OLD XXX + 30
675:#define PBE_SHA1 DES2_EDE_CBC_OLD XXX CKM_VENDOR_DEFINED_OLD XXX + 31
785:#define PKCS5_PBKD2 HMAC_SHA1 0x00000001
808:#define KDF 0x00000002
816:#define NIST KDF 0x00000012
823:#define SES KDF 0x82000000
835:#define KDF 0x00000003
836:#define SHA1 KDF CONCATENATE 0x00000004
838:#define SHA1 KDF CONCATENATE X9 42 CKD SHA1 KDF CONCATENATE
839:#define SHA1 KDF CONCATENATE NIST 0x80000001
841:#define SHA1 KDF CONCATENATE NIST X9 42 CKD SHA1 KDF ASN1 // not supported
842:#define SHA1 KDF CONCATENATE OLD XXX 0x80000002 // not supported
899:#define CMS HMAC_SHA1 0x00000001
900:#define CMS SHA1 0x00000002
954:#define MGF1 SHA1 0x00000001

Event: Commented out items in bitmap kerb_EncTypes
Message: /fipscc_nios/products/one/server/src/lib/msrpc/idl/security.idl:

413:// KERB_ENCTYPE_AES128_CTS_HMAC_SHA1_96 = 0x00000008,
414:// KERB_ENCTYPE_AES256_CTS_HMAC_SHA1_96 = 0x00000010

Event: Code to assign digest_algo in function ipki_regenerate_csr_from_db
Message: /fipscc_nios/products/one/server/src/lib/pki/ipki_api.c:

392: if (strcasecmp(csr.algorithm, "SHA-1") == 0)
393: digest_algo = IB_ALG_SHA1;

Event: Case of switch (a_digial) in function ipki_build_csr
Message: /fipscc_nios/products/one/server/src/lib/pki/ipki_gen.c:

823: case IB_ALG_SHA1:
824: IPKICALL(X509_REQ_sign(csr, a_key, EVP_sha1()));

**Event:** Case of switch (a_digest) in function ipki_create_selfsigned_cert  
**Message:**./fipscc_nios/products/one/server/src/lib/pki/ipki_gen.c:

```
1091: case IB_ALG_SHA1:
1092: IPKICALL(X509_sign(cert, privkey, EVP_sha1()));
```

**Event:** Argument of call X509_sign in function ipki_sign_cert  
**Message:**./fipscc_nios/products/one/server/src/lib/pki/ipki_gen.c:1189: IPKICALL(X509_sign(cert, privkey, EVP_sha1()));

**Event:** Argument of call X509_sign in function ipki_sign_cert  
**Message:**./fipscc_nios/products/one/server/src/lib/pki/ipki_gen.c:

```
1091: case IB_ALG_SHA1:
1092: IPKICALL(X509_sign(cert, privkey, EVP_sha1()));
```

**Event:** Comment to the module  
**Message:**./fipscc_nios/products/one/server/src/admin_conn/cookie.py:15:common hashes. Note that the recent vulnerabilities in md5 (and sha1)

**Event:** Module variables
**Message:**./fipscc_nios/products/one/server/src/admin_conn/cookie.py:

```
40:SHA1 = 'sha1'
45: _SHA1_LEN_B64 = 27
```

**Event:** Comments to class IBCookie  
**Message:**./fipscc_nios/products/one/server/src/admin_conn/cookie.py:

```
60: - The hmac is an md5 or sha1 hmac over the data and the salt,
61: md5, 27 chars for sha1). There is no separator between salt
```

**Event:** Code in function load  
**Message:**./fipscc_nios/products/one/server/src/admin_conn/cookie.py:

```
117: if len(cookie) - cookie.rfind(',') == _SHA1_LEN_B64 + _SALT_LEN_B64 + 1:
118: hlen = _SHA1_LEN_B64
119: hmactype = SHA1
```

**Event:** Assigning digestmod in function _hmac  
**Message:**./fipscc_nios/products/one/server/src/admin_conn/cookie.py:139: digestmod = hashlib.sha1 if hmactype == SHA1 else hashlib.md5

**Event:** Argument of call cookie.IBCookie in function _encode_ticket  
**Message:**./fipscc_nios/products/one/server/src/admin_conn/objcalls.py:1425: hmactype=cookie.SHA1)

**Event:** Argument of call cookie.IBCookie in function _decode_ticket  
**Message:**./fipscc_nios/products/one/server/src/admin_conn/objcalls.py:1431: c = cookie.IBCookie(hmactype=cookie.SHA1)

**Event:** Comments to the module  
**Message:**./fipscc_nios/products/one/server/src/admin_conn/cryptfuncs.py:13:# base64(<20 bytes sha1(password+salt)>

**Event:** Comments to function _getsshasalt  
**Message:**./fipscc_nios/products/one/server/src/admin_conn/cryptfuncs.py:48: "Extract the salt from a special IB sha1 passwd hash. hashepsw should be

**Event:** Comments to function _compute_ssha  
**Message:**./fipscc_nios/products/one/server/src/admin_conn/cryptfuncs.py:55: "Compute the special IB sha1 passwd hash, not including the prefix

**Event:** Function call hashlib.sha1 in function _compute_ssha  
**Message:**./fipscc_nios/products/one/server/src/admin_conn/cryptfuncs.py:57: h = hashlib.sha1(cleartpsw.encode('utf-8') + salt).digest()

**Event:** Import variable = SHA1= from module cookie  
**Message:**./fipscc_nios/products/one/server/src/admin_conn/userauth.py:42:from infoblox.one.admin_conn.cookie import (IBCokie, getsecret, SHA1,
Event: Assigning hmac type in function get_cookie
Message: ./fipsc_nios/products/one/server/src/admin_conn/userauth.py:346: hmac type = SHA1

Event: Assigning hmac type in function _check_cookie
Message: ./fipsc_nios/products/one/server/src/admin_conn/userauth.py:
   1144: hmac type = SHA1
   1150: hmac type = SHA1

Event: Commented out item in list TSIG_KEY_ALGORITHMS
Message: ./fipsc_nios/products/one/server/src/admin_conn/objtype.py:124:'HMAC-SHA1',

Event: Comment in PagingPageID.__init__
Message: ./fipsc_nios/products/one/server/src/admin_conn/wapibase.py:1041: Create a paging cookie container, it will use SHA1

Event: Argument of call hmac.HMAC in function _hmac
Message: ./fipsc_nios/products/one/server/src/admin_conn/wapibase.py:1068: h = hmac.HMAC(self.secret, msg=data, digestmod=hashlib.sha1)

Event: Assign hmac type in function generateIAC which generates extended time cookie for PAPI jobs from NetMRI
Message: ./fipsc_nios/products/one/server/src/pyutil/tae_util.py:476: hmac type = 'sha1'

Event: Part of the code to verify the private key matches the public key in the certificate in function _check_join_info
Message: ./fipsc_nios/products/one/server/src/pyutil/subgrid.py:
   140: signature = RSA_key_pair.sign(digest, 'sha1')
   143: if user_pub_rsa.verify(digest, signature, 'sha1') != 1:

Event: Assign local variable digest_algo in function util_generate_and_encode_csr
Message: ./fipsc_nios/products/one/server/src/pyutil/ibutil.c:5917: IB_DIGEST_ALGORITHM digest_algo = IB_ALG_SHA1;

Event: Assign local variable digest_algo in function util_sign_csr
Message: ./fipsc_nios/products/one/server/src/pyutil/ibutil.c:6086: IB_DIGEST_ALGORITHM digest_algo = IB_ALG_SHA1;

Event: Authentication type mapping for one.bfd_template
Message: ./fipsc_nios/products/one/server/src/pyutil/installdb_mappings.py:
   1603: 'sha1': 'SHA1',
   1604: 'meticulous-sha1': 'METICULOUS-SHA1',

Event: Comment to function _set_old_default_grid_dnssec_algorithm
Message: ./fipsc_nios/products/one/server/src/pyutil/testutils/dnssec_test_mixin.py:372: Set grid level DNSSEC algorithm to RSASHA1

Event: Arguments of function call self._change_grid_dnssec_settings
Message: ./fipsc_nios/products/one/server/src/pyutil/testutils/dnssec_test_mixin.py:
   378: self._change_grid_dnssec_settings(ksk_algorithm='RSASHA1',
   379: zsk_algorithm='RSASHA1',

Event: Item of enumlist of field algorithm in class WAPIStruct_dnssec_algorithm_2_0
Message: ./fipsc_nios/products/one/server/src/wapi/grid.py:118: enumlist=["RSAMD5", 'DSA', 'RSASHA1', 'RSASHA256',

Event: Assign algorithm type in WFEnumAlgorithm.w2i
Message: ./fipsc_nios/products/one/server/src/wapi/grid.py:
   155: algorithm = 'RSASHA1'
   161: algorithm = 'RSASHA1'

Event: Assign algorithm type in WFEnumAlgorithm.i2w
Message: ./fipsc_nios/products/one/server/src/wapi/grid.py:180: elif algorithm == 'RSASHA1'.
Event: Item of enumlist of field algorithm in class WAPIStruct_generatecsr_2_6
Message: /fipscc_nios/products/one/server/src/wapi/fileops.py:2651: enumlist=['SHA-1', 'SHA-256'],

Event: Dictionary of possible authentication types in NIOS WAPI for BFD
Message: /fipscc_nios/products/one/server/src/wapi/bfdtemplate.py:44: enumlist=['NONE', 'MD5', 'METICULOUS-MD5', 'SHA1'],

Event: Dictionary of possible authentication types in NIOS IBAP for BFD
Message: /fipscc_nios/products/one/server/src/wapi/bfdtemplate.py:45: 'METICULOUS-SHA1',

Event: Item of list SFNT_SIG_ALGORITHMS
Message: /fipscc_nios/products/one/server/src/pyabs/one_include.py:460:SFNT_SIG_ALGORITHMS = ['RSASHA1', 'RSASHA256']

Event: Item of list ONE_SIG_ALGORITHMS
Message: /fipscc_nios/products/one/server/src/pyabs/one_include.py:461:ONE_SIG_ALGORITHMS = ['SHA-1', 'SHA-256']

Event: Item of dictionary HSM_VER_SIGN_DICT
Message: /fipscc_nios/products/one/server/src/pyabs/hsm_safenet_group.py:91:HSM_VER_SIGN_DICT = {'LunaSA_4': 'sha1WithRSAEncryption'}

Event: Setting db_algorithm and digest in function insert
Message: /fipscc_nios/products/one/server/src/pyabs/self_signed_cert.py:
  88: elif self['algorithm'] in ('RSASHA1', 'SHA-1'):
  89: db_algorithm = 'SHA-1'
  90: digest = 'sha1'

Event: Assign default algorithm type in function one_assign_self_signed_certificate
Message: /fipscc_nios/products/one/server/src/pyabs/certificate.py:243: algorithm = "RSASHA1"

Event: Check key size and algorithm type in function generate_csr
Message: /fipscc_nios/products/one/server/src/pyabs/certificate.py:1045: (args['key_size'] == 4096 and args['algorithm'] == 'SHA-1'):

Event: Setting algorithm type in function generate_csr
Message: /fipscc_nios/products/one/server/src/pyabs/certificate.py:1053: args['algorithm'] = 'SHA-1'

Event: Check key size and algorithm type in function generate_self_signed_cert
Message: /fipscc_nios/products/one/server/src/pyabs/certificate.py:1102: (args['key_size'] == 4096 and args['algorithm'] == 'SHA-1'):

Event: Setting algorithm type in function generate_self_signed_cert
Message: /fipscc_nios/products/one/server/src/pyabs/certificate.py:1110: args['algorithm'] = 'SHA-1'

Event: Key length definition
Message: /fipscc_nios/products/one/server/src/bin/ib_prngd/main.c:36:#define RESULT_LEN 20 // As per hash engine, i.e. SHA1 needs 20 characters. Moreover, SP 800-90A suggests 160 bits either

Event: Comments to function hmac_sha1
Message: /fipscc_nios/products/one/server/src/bin/ib_prngd/main.c:
  463: * SHA-1 in one go. It will make all of the other much easier to read.
  467: * @param a_output (ib_dstring *) output to return the result back to caller, for SHA-1 it must be 20 characters of length

Event: Definition of function hmac_sha1
Message: /fipscc_nios/products/one/server/src/bin/ib_prngd/main.c:472:hmac_sha1(const ib_dstring *a_key, const ib_dstring *a_v, ib_dstring *a_output)

Event: Call of EVP_sha1() in function hmac_sha1
Message: /fipscc_nios/products/one/server/src/bin/ib_prngd/main.c:486: HMAC_Init_ex(&ctx, a_key->m_str, a_key->m_len, EVP_sha1(), NULL);

Event: Call of hmac_sha1 in function hmac_drbg_update
Message:/fipscc_nios/products/one/server/src/bin/ib_prngd/main.c:

538: ICALL(hmac_sha1(key, buf, key));
545: ICALL(hmac_sha1(key, v, v));
562: ICALL(hmac_sha1(key, buf, key));
568: ICALL(hmac_sha1(key, v, v));

Event: Call of hmac_sha1 in function hmac_drbg_generate
Message:/fipscc_nios/products/one/server/src/bin/ib_prngd/main.c:773: ICALL(hmac_sha1(key, v, v_out));

Event: TBD comment in function main
Message:/fipscc_nios/products/one/server/src/bin/ib_prngd/main.c:1086: "Suggested to just concatenate (i.e. use buf, no hmac_sha1) and send to instantiate.

Event: Items of enum ssh_macs_setting_t
Message:/fipscc_nios/products/one/server/src/bin/make_sshd_conf/main.c:

31: SSH_SHA1 = 1,
32: SSH_SHA1_ETM = 2,

Event: Item of mapping tls_ssh_mapping_t g_macs_mapping[]
Message:/fipscc_nios/products/one/server/src/bin/make_sshd_conf/main.c:76: {"SHA", "hmac-sha1,hmac-sha1-etm@openssh.com", SSH_SHA1 | SSH_SHA1_ETM},

Event: Argument of function ipki_generate_csr
Message:/fipscc_nios/products/one/server/src/bin/make_default_apache_cert/main.c:163: a_data->m_db_pool, &name_list,
IB_IPKI_PUB_KEY_SIZE_2048, IB_ALG_SHA1,

Event: Argument of function ipki_create_selfsigned_cert
Message:/fipscc_nios/products/one/server/src/bin/make_default_apache_cert/main.c:167: a_data->m_db_pool, IB_ALG_SHA1, NULL,

Event: Check optarg to set usage_flag in function mhc_process_command_line
Message:/fipscc_nios/products/one/server/src/bin/sfnt_client_cert_changed/main.c:86: if (strcmp(optarg, "RSASHA1") &&

Event: Print usage in function mhc_process_command_line
Message:/fipscc_nios/products/one/server/src/bin/sfnt_client_cert_changed/main.c:116: fprintf (stderr, "Usage: %s -a ",

Event: Mechanism types
Message:/fipscc_nios/products/one/server/src/bin/show_safenet_keylabel/e_gem.h:

72:#define CKM_SHA1_RSA_PKCS 0x00000006
74:#define CKM_SHA1_RSA_X9_31 0x0000000C
84:#define CKM_ECDSA_SHA1 0x00001042

Event: Attribute type
Message:/fipscc_nios/products/one/server/src/bin/show_safenet_keylabel/e_gem.h:152:#define CKA_FINGERPRINT_SHA1
(CKA_VENDOR_DEFINED | 0x0002)

Event: Definition for OAEP
Message:/fipscc_nios/products/one/server/src/bin/show_safenet_keylabel/e_gem.h:601:#define CKM_MGF1_SHA1 0x00000001

Event: The argument of command /usr/sbin/openvpn in function cd_start_replica_vpn
Message:/fipscc_nios/products/one/server/src/bin/clusterd/util.c:3452: args[argc++] = "SHA1";

Event: The argument of command /usr/sbin/openvpn in function cd_start_master_vpn
Message:/fipscc_nios/products/one/server/src/bin/clusterd/util.c:3636: args[argc++] = "SHA1";

Event: Part of the code to derive a serial number from a string in function cd_derive_serial
Message:/fipscc_nios/products/one/server/src/bin/clusterd/util.c:4915: ITEST(EVP_DigestInit(&ctx, EVP_sha1()) == 1, IERR_FAILURE);

Event: Setting options in CC mode
Message: `/fipscc_nios/products/one/server/src/bin/util/upload_backup_scp.pl`:

76: $options .= ' -o MACs=hmac-sha1,hmac-sha1-96,hmac-md5,hmac-md5-96';
77: $options .= ' -o KexAlgorithms=diffie-hellman-group14-sha1';

Event: Item in dictionary SFNET_FACT_CONF_DICT - backup configuration file name
Message: `/fipscc_nios/products/one/server/src/bin/util/hsm_safenet_reset_client_cert.py:14:` ‘RSASHA1’:

Event: Setting options in CC mode
Message: `/fipscc_nios/products/one/server/src/bin/util/download_hotfix_scp.pl`:

74: $options .= ' -o MACs=hmac-sha1,hmac-sha1-96,hmac-md5,hmac-md5-96';
75: $options .= ' -o KexAlgorithms=diffie-hellman-group14-sha1';

Event: Input parameters
Message: `/fipscc_nios/products/one/server/src/bin/util/hsm_safenet_generate_client_cert.sh:12:` $1: RSASHA1 | RSASHA256

Event: Check type of the input parameter
Message: `/fipscc_nios/products/one/server/src/bin/util/hsm_safenet_generate_client_cert.sh:21:` if [ "$1" == “RSASHA1” ];

Event: Check type of the input parameter
Message: `/fipscc_nios/products/one/server/src/bin/util/hsm_safenet_generate_client_cert.sh:72:` if [ "$1" == “RSASHA1” ];

Event: Print GSSD encrypt types in function show_dns_gss_tsig_counters
Message: `/fipscc_nios/products/one/server/src/bin/serial_console/show.c`:

10245: PCRYPTO("aes128-cts-hmac-sha1-96", GSSD_ETYPE_AES128_CTS_HMAC_SHA1_96);
10246: PCRYPTO("aes256-cts-hmac-sha1-96", GSSD_ETYPE_AES256_CTS_HMAC_SHA1_96);

Event: Item of enum IB_DIGEST_ALGORITHM
Message: `/fipscc_nios/products/one/server/include/infoblox/one/ipki_gen.h:118:` IB_ALG_SHA1, ...

Event: Create public key in function create_temp_cert

Event: Create sign key in function create_temp_cert
Message: `/fipscc_nios/products/gog/server/src/pyutil/cert_util.py:355:` sign_key = M2Crypto.EVP.PKey(md='sha1')

Event: Sign X509 certificate request in function m2_generate_and_encode_csr

Event: Sign X509 certificate in function m2_create_cert_and_sign
Message: `/fipscc_nios/products/gog/server/src/pyutil/cert_util.py:450:` cert.sign(sign_key, 'sha1')

Event: The argument of command `/usr/sbin/openvpn` in function anp_vpn_client

Event: The argument of command `/usr/sbin/openvpn` in function anm_vpn_server

Event: Assigning authentication protocol in function snmp_task_data_init
Message: `/fipscc_nios/products/bind/server/src/bin/idns_healthd/snmp_monitor.c:752:` ss.securityAuthProto = usmHMACHS1AuthProtocol;

Event: Cases of switch ((unsigned int)mech) in function const char *NFC_mechanism2name(CK_MECHANISM_TYPE mech), macros M: #define M(MECH) case MECH: return #MECH
Message: `/fipscc_nios/products/dns/server/src/lib/thales_preload/ckerrcode.c`:

259:#ifndef CKM_SHA1_RSA_PKCS
260: M(CKM_SHA1_RSA_PKCS);
277:#ifndef CKM_SHA1_RSA_X9_31
278: M(CKM_SHA1_RSA_X9_31);
283: #ifdef CKM_SHA1_RSA_PKCS_PSS
284: M(CKM_SHA1_RSA_PKCS_PSS);
292: #ifdef CKM_DSA_SHA1
293: M(CKM_DSA_SHA1);
643: #ifdef CKM_SSL3_SHA1_MAC
644: M(CKM_SSL3_SHA1_MAC);
652: #ifdef CKM_SHA1_KEY_DERIVATION
653: M(CKM_SHA1_KEY_DERIVATION);
679: #ifdef CKM_PBE_SHA1_CAST128_CBC
680: M(CKM_PBE_SHA1_CAST128_CBC);
682: #ifdef CKM_PBE_SHA1_DES3_EDE_CBC
683: M(CKM_PBE_SHA1_DES3_EDE_CBC);
685: #ifdef CKM_PBE_SHA1_DES2_EDE_CBC
686: M(CKM_PBE_SHA1_DES2_EDE_CBC);
688: #ifdef CKM_PBE_SHA1_RC2_128_CBC
689: M(CKM_PBE_SHA1_RC2_128_CBC);
691: #ifdef CKM_PBE_SHA1_RC2_40_CBC
692: M(CKM_PBE_SHA1_RC2_40_CBC);
697: #ifdef CKM_PBA_SHA1_WITH_SHA1_HMAC
698: M(CKM_PBA_SHA1_WITH_SHA1_HMAC);
796: #ifdef CKM_KCDSA_SHA1
797: M(CKM_KCDSA_SHA1);
884: M(CKM_PBE_SHA1_ARCFOUR_128);
885: M(CKM_PBE_SHA1_ARCFOUR_40);
890: M(CKM_PBE_SHA1_RC4_128);
918: case CKM_KCDSA_SHA1:
919: return "CKM_KCDSA_SHA1";

Event: Constant definition
Message: ./fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/pkcs11/pkcs11extra.h:58:#define CKM_KCDSA_SHA1 (CKM_NCIPHER + 0x4UL)

Event: Constant definition
Message: ./fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/pkcs11/pkcs11extra.h:

168: #ifndef CKD_SHA1_KDF
182: #define CKD_SHA1_KDF 0x00000002

Event: Thales sources comment
Message: ./fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/pkcs11/pkcs11extra.h:637:" CKM_MD2_RSA_PKCS, CKM_MD5_RSA_PKCS, and CKM_SHA1_RSA_PKCS

Event: Constant definition
Message: ./fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/pkcs11/pkcs11t.h:641:#define CKM_SHA1_RSA_PKCS 0x00000006

Event: Thales sources comment
Message: ./fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/pkcs11/pkcs11t.h:649:" CKM_RSA_X9_31_KEYPAIRGEN, CKM_RSA_X9_31_CBC, CKM_SHA1_RSA_X9_31,

Event: Thales sources comment
Message: ./fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/pkcs11/pkcs11t.h:650: * CKM_RSA_PKCS_PSS, and CKM_SHA1_RSA_PKCS_PSS are new for v2.11 */

Event: Constant definitions
Message: ./fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/pkcs11/pkcs11t.h:

653: #define CKM_SHA1_RSA_X9_31 0x0000000C
655: #define CKM_SHA1_RSA_PKCS_PSS 0x0000000E
659: #define CKM_DSA_SHA1 0x00000012
845: #define CKM_PBE_SHA1_CAST5_CBC 0x000003A5
864: #define CKM_PBE_SHA1_CAST128_CBC 0x000003A5
865: #define CKM_PBE_SHA1_RC2_128_CBC 0x000003A6
867: #define CKM_PBE_SHA1_RC4_40 0x000003A7

Copyright ©2019, Infoblox, Inc. All right reserved.
Event: Items of enum M_KeyType and comments to them

Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-en.h:

1251: ** by hashing seed using SHA-1 to generate q. For other
1280: /* A key usable with the HMACSHA1 mechanism
1282: * See \ref KeyType_HMACSHA1 for more information.
1284: * KeyType_HMACSHA1 = 27,
1487: ** a hash algorithm other than SHA-1.

Event: Items of enum M_Mech and comments to them

Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-en.h:

1590: ** plaintext. A Bytes plaintext is hashed using SHA-1 before
1631: /* The SHA-1 hash function as standardized in FIPS180-1
1633: * See \ref Mech_SHA1Hash for more information.
1635: * Mech_SHA1Hash = 44,
1651: /* The HMAC construction using the SHA-1 hash function
1653: * See \ref Mech_HMACSHA1 for more information.
1655: * Mech_HMACSHA1 = 55,
1678: ** A Bytes plaintext is hashed using SHA-1 to form a Hash plaintext. A
1683: * See \ref Mech_RSAhSHA1pPKCS1 for more information.
1685: Mech_RSAhSHA1pPKCS1 = 59,
1689: ** A Bytes plaintext is hashed using SHA-1 to form a Hash plaintext. A
1698: ** MGF1 with SHA-1 is used as the mask generation function.
1800: Mech_DES3wSHA1 = 102,
1811: Mech_KCEDASHA1 = 111,
1827: ** - KDF2 key derivation function, using SHA-1 as the underlying hash function
1828: ** - Triple-DES-CBC-IV0 with 24-byte keys (@ref Mech_DLIESe3DEShSHA1) as the symmetric
1830: ** - MAC1 based on SHA-1 as the message authentication scheme, with 160-bit output
1833: * See \ref Mech_DLIESe3DEShSHA1 for more information.
1835: Mech_DLIESe3DEShSHA1 = 124,
1839: ** - KDF2 key derivation function, using SHA-1 as the underlying hash function
1840: ** - AES256-CBC-IV0 with 16-byte keys (@ref Mech_DLIESeAEShSHA1) as the symmetric
1842: ** - MAC1 based on SHA-1 as the message authentication scheme, with 160-bit output
1845: * See \ref Mech_DLIESeAEShSHA1 for more information.
1847: Mech_DLIESeAEShSHA1 = 125,
1871: Mech_BlobCrypt2kHashesRijndaelCBC0SHA1mSHA1HMAC = 141,
1872: Mech_BlobCrypt2kRSAeRijndaelCBC0SHA1mSHA1HMAC = 142,
1875: Mech_BlobCrypt2kDHeRijndaelCBC0SHA1mSHA1HMAC = 143,
1876: Mech_BlobCrypt2kHashesDES3CBC0SHA1mSHA1HMAC = 145,
1876: Mech_BlobEncrypt2kRSAeDES3CBC0SHA1mSHA1HMAC = 146,
1877: Mech_BlobEncrypt2kDHeDES3CBC0SHA1mSHA1HMAC = 147,
1885: ** or Bytes plaintext. A Bytes plaintext is hashed using SHA-1 before
1907: ** or Hash plaintext. A Bytes plaintext is hashed using SHA-1.
1908: ** SHA-1 is also used for mask generation. This mechanism assumes a
1914: * See \ref Mech_RSAhSHA1pPSS for more information.
1916: Mech_RSAhSHA1pPSS = 160,
** 

`/** 

* The HMAC construction using the SHA-1 hash function
*/

`/** 

* A Bytes plaintext is hashed using SHA-1 to form a Hash plaintext. 
*/

`/** 

* A Bytes plaintext is hashed using SHA-1 to form a Hash plaintext. 
*/

`/** 

* SHA-1 is also used for mask generation. This mechanism assumes a 
*/

8669: ** default of SHA-1. */

`/** 

* or Bytes plaintext. A Bytes plaintext is hashed using SHA-1 before 
*/

`/** 

* SHA-1 based on SHA-1 as the message authentication scheme, with 160-bit output 
*/

`/** 

* SHA-1 as the message authentication scheme, with 160-bit output 
*/

`/** 

* SHA-1 as the underlying hash function 
*/

`/** 

* SHA-1 as the underlying hash function 
*/

`/** 

* SHA-1 as the underlying hash function 
*/

`/** 

* SHA-1 as the underlying hash function 
*/

`/** 

* SHA-1 as the underlying hash function 
*/

`/** 

* SHA-1 as the underlying hash function 
*/

`/** 

* SHA-1 as the underlying hash function 
*/

`/** 

* SHA-1 as the underlying hash function 
*/

`/** 

* SHA-1 as the underlying hash function 
*/

`/** 

* SHA-1 as the underlying hash function 
*/

`/** 

* SHA-1 as the underlying hash function 
*/

```c
#define KDPKeyType_HMACSHA1 161
```
SHA-1.

Event: Comments to struct M_KeyType_DSACommGenParams
Message://ipsc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:1602: ** by hashing seed using SHA-1 to generate q. Other

Event: Comments to struct M_KeyType_Random_Data
Message://ipsc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:1887: * This is the variant of `ref M_KeyType__Data chosen where the tag is any of `ref KeyType_Random, `ref KeyType_ArcFour, `ref KeyType_CAST, `ref KeyType_Wrapped, `ref KeyType_HMACMD5, `ref KeyType_HMACSHA1, `ref KeyType_HMACRIPEMD160, `ref KeyType_Serpent, `ref KeyType_Rijndael, `ref KeyType_Twofish, `ref KeyType_CAST256, `ref KeyType_Blowfish, `ref KeyType_HMACSHA224, `ref KeyType_HMACSHA256, `ref KeyType_HMACSHA384, `ref KeyType_HMACSHA512, `ref KeyType_HMACTiger, `ref KeyType_SEED, `ref KeyType_ARIA or `ref KeyType_Camellia.

Event: Comments to struct M_KeyType_DSACommVariableSeed_Data
Message://ipsc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:1940: ** a hash algorithm other than SHA-1.

Event: Comments to struct M_KeyType_DSAComm_Data
Message://ipsc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:2132: ** by hashing seed using SHA-1 to generate q.

Event: Comments to struct M_Mech_RSApPKCS1OAEP_IV
Message://ipsc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:2408: ** MGF1 with SHA-1 is used as the mask generation function.

Event: Comments to struct M_Mech_DSA_Cipher
Message://ipsc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:2625: ** plaintext. A Bytes plaintext is hashed using SHA-1 before

Event: Comment to typedef struct M_Mech_DLIESe3DEShSHA1_Cipher M_Mech_DLIESe3DEShSHA1_Cipher;
Message://ipsc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:2678;" --- Structure Mech_DLIESe3DEShSHA1_Cipher --- */

Event: type M_Mech_DLIESe3DEShSHA1_Cipher; definition
Message://ipsc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:2680:typedef struct
M_Mech_DLIESe3DEShSHA1_Cipher M_Mech_DLIESe3DEShSHA1_Cipher;

Event: Comments to struct M_Mech_DLIESe3DEShSHA1_Cipher
Message://ipsc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:2682;" --- Structure Mech_DLIESe3DEShSHA1_Cipher --- */
2684;"/addtogroup Mech_DLIESe3DEShSHA1
2691; ** KDF2 key derivation function, using SHA-1 as the underlying hash function
2692; ** Triple-DES-CBC-IV0 with 24-byte keys (@ref Mech_DLIESe3DEShSHA1) as the symmetric
2694; ** MAC1 based on SHA-1 as the message authentication scheme, with 160-bit output
2697; * This is the variant of `ref M_Mech__Cipher chosen where the tag is either `ref Mech_DLIESe3DEShSHA1 or `ref Mech_DLIESeAEShSHA1.

Event: struct M_Mech_DLIESe3DEShSHA1_Cipher definition
Message://ipsc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:2699:struct
M_Mech_DLIESe3DEShSHA1_Cipher {

Event: Field of struct M_Mech_SSL3FinishedMsg_Cipher
Message://ipsc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:2792: M_Hash20 sha1hash;

Event: Comment to struct M_Mech_ECDSA_Cipher
Message://ipsc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:2909: ** or Bytes plaintext. A Bytes plaintext is hashed using SHA-1 before

Event: Comment to typedef struct M_Mech_SHA1Hash_Cipher M_Mech_SHA1Hash_Cipher;
Message://ipsc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:3092;" --- Structure
Mech_SHA1Hash_Cipher --- */

**Event:** type M_Mech_SHA1Hash_Cipher definition
**Message:** /fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:3094:typedef struct M_Mech_SHA1Hash_Cipher M_Mech_SHA1Hash_Cipher;

**Event:** Comments to struct M_Mech_SHA1Hash_Cipher
**Message:** /fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:3096:/* --- Structure Mech_SHA1Hash_Cipher --- */
3098:** The SHA-1 hash function as standardized in FIPS180-1
3102:** This is the variant of \
ref Mech_SHA1Hash chosen where the tag is either \ref Mech_SHA1Hash or \ref Mech_HMACSHA1.

**Event:** struct M_Mech_SHA1Hash_Cipher definition
**Message:** /fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:3106:struct M_Mech_SHA1Hash_Cipher
{

**Event:** Fields of union M_Mech___Cipher and comments to them
**Message:** /fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:
3127: /** if tag is \ref Mech_DLIESe3DEShSHA1 */
3128: M_Mech_DLIESe3DEShSHA1_Cipher dliese3deshsha1;
3183: /** if tag is \ref Mech_SHA1Hash */
3184: M_Mech_SHA1Hash_Cipher sha1hash;

**Event:** Comment to field M_Mech kdfhash; of struct M_DeriveMech_ECCMQV_DKParams
**Message:** /fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-im.h:4039: ** Supported mechanisms are SHA1Hash, SHA24Hash,

**Event:** Comment to const KeyType_DSAComm definition
**Message:** /fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1140: ** by hashing seed using SHA-1 to generate q.

**Event:** Const KeyType_HMACSHA1 definition with comments
**Message:** /fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:
1169: /** A key usable with the HMACSHA1 mechanism
1171: * See \ref KeyType_HMACSHA1 for more information.
1173:#define KeyType_HMACSHA1 27

**Event:** Comment to const KeyType_DSACommVariableSeed definition
**Message:** /fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1376: ** a hash algorithm other than SHA-1.

**Event:** Comment to const Mech_DSA definition (Digital Signature Algorithm)
**Message:** /fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1446: ** plaintext. A Bytes plaintext is hashed using SHA-1 before

**Event:** Const Mech_SHA1Hash definition with comments
**Message:** /fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:
1487: /** The SHA-1 hash function as standardized in FIPS180-1
1489: * See \ref Mech_SHA1Hash for more information.
#define Mech_SHA1Hash 44

**Event:** Const Mech_HMACSHA1 definition with comments
**Message:** /fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:
1507: /** The HMAC construction using the SHA-1 hash function
1509: * See \ref Mech_HMACSHA1 for more information.
1511:#define Mech_HMACSHA1 55
Event: Const Mech_RSAhSHA1pPKCS1 definition with comments
Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:
1534: ** A Bytes plaintext is hashed using SHA-1 to form a Hash plaintext. A
1539: * See \ref Mech_RSAhSHA1pPKCS1 for more information.
1541:#define Mech_RSAhSHA1pPKCS1 59

Event: Comment to const Mech_RSAhRIPEMD160pPKCS1 definition
Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1545: ** A Bytes plaintext is hashed using SHA-1 to form a Hash plaintext.

Event: Comment to const Mech_RSApPKCS1OAEP definition
Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1554: ** MGF1 with SHA-1 is used as the mask generation function.

Event: Const Mech_DES3wSHA1 definition
Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1656:#define Mech_DES3wSHA1 102

Event: Const Mech_KCDSASHA1 definition
Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1667:#define Mech_KCDSASHA1 111

Event: Const Mech_DLIESe3DES SHA1 definition with comments
Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:
1683: ** - KDF2 key derivation function, using SHA-1 as the underlying hash function
1684: ** - Triple-DES-CBC-IV0 with 24-byte keys (@ref Mech_DLIESe3DES SHA1) as the symmetric
1686: ** - MAC1 based on SHA-1 as the message authentication scheme, with 160-bit output
1689: * See \ref Mech_DLIESe3DES SHA1 for more information.
1691:#define Mech_DLIESe3DES SHA1 124

Event: Const Mech_DLIESeAEShSHA1 definition with comments
Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:
1695: ** - KDF2 key derivation function, using SHA-1 as the underlying hash function
1696: ** - AES256-CBC-IV0 with 16-byte keys (@ref Mech_DLIESeAEShSHA1) as the symmetric
1698: ** - MAC1 based on SHA-1 as the message authentication scheme, with 160-bit output
1701: * See \ref Mech_DLIESeAEShSHA1 for more information.
1703:#define Mech_DLIESeAEShSHA1 125

Event: Const Mech_BlobCryptv2kHasherRijndaelCBC0hSHA1mSHA1HMAC definition
Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1727:#define Mech_BlobCryptv2kHasherRijndaelCBC0hSHA1mSHA1HMAC 141

Event: Const Mech_BlobCryptv2kRSAeRijndaelCBC0hSHA1mSHA1HMAC definition
Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1728:#define Mech_BlobCryptv2kRSAeRijndaelCBC0hSHA1mSHA1HMAC 142

Event: Const Mech_BlobCryptv2kDHeRijndaelCBC0hSHA1mSHA1HMAC definition
Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1729:#define Mech_BlobCryptv2kDHeRijndaelCBC0hSHA1mSHA1HMAC 143

Event: Const Mech_BlobCryptv2kHasheDES3CBC0hSHA1mSHA1HMAC definition
Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1731:#define Mech_BlobCryptv2kHasheDES3CBC0hSHA1mSHA1HMAC 145

Event: Const Mech_BlobCryptv2kRSAeDES3CBC0hSHA1mSHA1HMAC definition
Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1732:#define Mech_BlobCryptv2kRSAeDES3CBC0hSHA1mSHA1HMAC 146

Event: Const Mech_BlobCryptv2kDHeDES3CBC0hSHA1mSHA1HMAC definition
Message:/fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1733:#define Mech_BlobCryptv2kDHeDES3CBC0hSHA1mSHA1HMAC 147
Event: Comments to const Mech_ECDSA definition
Message:./fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:1741: ** or Bytes plaintext. A Bytes plaintext is hashed using SHA-1 before

Event: Const Mech_RSAhSHA1pPSS definition with comments
Message:./fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:
   1763: ** or Hash plaintext. A Bytes plaintext is hashed using SHA-1.
   1764: ** SHA-1 is also used for mask generation. This mechanism assumes a
   1770: * See 'ref Mech_RSAhSHA1pPSS for more information.
   1772:#define Mech_RSAhSHA1pPSS 160

Event: Comment to const KeyType_DSAPrivate_GenParams_flags_qhash_present definition
Message:./fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:4438: ** default of SHA-1. */

Event: Comments to Data structure formats
Message:./fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/messages-a-dh.h:
   6578: * CIPHER for Mech = DLIESe3DESShSHA1
   6595: * HASH20 sha1hash
   6668: * CIPHER for Mech = SHA1Hash
   9244: * IV for Mech = BlobCryptv2kHasheDES3CBC0hSHA1mSHA1HMAC
   9245: * IV for Mech = KCDSHA1A
   9252: * IV for Mech = RSAhSHA1pPKCS1
   9258: * IV for Mech = BlobCryptv2kRSAeRijndaelCBC0hSHA1mSHA1HMAC
   9271: * IV for Mech = DES3wSHA1
   9274: * IV for Mech = DLIES3DESShSHA1
   9284: * IV for Mech = HMACSHA1
   9297: * IV for Mech = DLIESAEShSHA1
   9324: * IV for Mech = BlobCryptv2kHasheRijndaelCBC0hSHA1mSHA1HMAC
   9326: * IV for Mech = RSAhSHA1pPSS
   9335: * IV for Mech = BlobCryptv2kDHeDES3CBC0hSHA1mSHA1HMAC
   9345: * IV for Mech = SHA1Hash
   9346: * IV for Mech = BlobCryptv2kDHeRijndaelCBC0hSHA1mSHA1HMAC
   9348: * IV for Mech = BlobCryptv2kRSAeDES3CBC0hSHA1mSHA1HMAC
   9354: * IV for Mech = SHA1Hash

Event: Comment to function NCH_hexout - Marshaled-hex format routine
Message:./fipscc_nios/products/dns/server/src/lib/thales_preload/thales/include/hilibs/stdmarshal.h:122:/* Note, if you use these, you must link against the nfast SHA1 implementation;

Event: Options returned by function algname
Message:./fipscc_nios/products/dns/server/src/lib/dnsdb/zone.c:
   112: return ("(RSASHA1)"):
   116: return ("(NSEC3RSASHA1)"):

Event: Items of dictionary enctype_enummap
Message:./fipscc_nios/products/dns/server/src/wapi/kerberoskey.py:
   16: 'AES256-CTS-HMAC-SHA1-96': 'aes256-cts-hmac-sha1-96',

Event: Items of dictionary DNSSEC_ALGORITHM_MNEMONICS
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:62:# algorithms are for internal use only, and DSA and RSASHA1 will
be converted
   108: '5' : {' 5', 'RSASHA1', 'RSA/SHA-1'},
   110: '7' : {' 7', 'NSEC3RSASHA1', 'RSA/SHA-1/NSEC3'},

Event: Comments to list SUPPORTED_ALGORITHMS
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:64:SUPPORTED_ALGORITHMS = ['RSAMD5', 'DSA', 'RSASHA1', 
Items of ALGORITHMS_NAME_DICT

Event: Items of ALGORITHMS_NAME_DICT
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py: 

71: '5': 'RSASHA1',
73: '7': 'NSEC3RSASHA1',

Event: Item of DIGEST_TYPES_NAME_DICT
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:83: DIGEST_TYPES_NAME_DICT = { '1': 'SHA_1',

Event: digest_sha1=True is argument of function gen_key_file_and_ds_record which puts the DNSKEY record information into a file, it is called in function common_generate_ds_record
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:765: digest_sha1=True,

Event: digest_sha1=True is the argument of function gen_dsrecord_from_dnskey which generates DSRecord file from DNS key
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:821: def gen_dsrecord_from_dnskey(input_file, output_file, digest_sha1=True,

Event: Using argument digest_sha1 of function gen_dsrecord_from_dnskey
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:826: if digest_sha1 and digest_sha256:

Event: digest_sha1=True is the argument of function gen_dsrecord_from_dnskey which generates DSRecord file from DNS key
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:851: def gen_key_file_and_ds_record(fqdn, obj, output_file, digest_sha1=True,

Event: Using digest_sha1 as the argument of function gen_dsrecord_from_dnskey which generates DSRecord file from DNS key
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:866: gen_dsrecord_from_dnskey(dnskey_file, output_file, digest_sha1,

Event: Comments to function common_validate_algorithm_size
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:1161: ''' Only are RSASHA1 NSEC3RSASHA1 RSASHA256 RSASHA512 approved in CC mode

Event: Comments to function common_validate_algorithm_size_obj
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:1193: Only are RSASHA1 NSEC3RSASHA1 RSASHA256 RSASHA512 approved in CC mode

Event: Comments to function DnsSecKeyReader.import_keys
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:1404: Algorithm: 5 (RSASHA1)

Event: Comments in function DnsSecKeyReader._read_private_key
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:1529: m = re.match('(\d+).+', algorithm_str) # e.g. "5 (RSASHA1)"

Event: Comments to function DnsSecKeyWriter.export_keypairs
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:1640: Algorithm: 5 (RSASHA1)

Event: Item in conversion table ui_to_internal in function validate_algorithms_and_convert
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:4326: '5': 'RSASHA1',

Event: Comment in function validate_algorithms_and_convert
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py:4374: # Convert DSA and RSASHA1 to NSEC3 versions if NSEC3 selected

Event: Items in conversion table for Internal->UI conversion num_to_str in function get_synthetic_algorithms_field
Message:./fipscc_nios/products/dns/server/src/pyabs/dnssec_common.py: 4402: '5': 'RSASHA1',
4404: '7': 'RSASHA1',

Event: Comments in function get_algorithms_namesize_strings
List of NIOS Algorithms

This section describes the cryptography, such as openssl and custom code, that the NIOS modules use.

<table>
<thead>
<tr>
<th>Name</th>
<th>Anchor (Line number, File Name and etc)</th>
<th>Cryptography items description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>A config maker, cipher suites are configurable via serial console</td>
<td>OpenSSL C-functions</td>
</tr>
<tr>
<td></td>
<td>SSL options are made available in below conf files like SSLCipherSuite, SSLCertificateFile, SSLCertificateKeyFile etc</td>
<td></td>
</tr>
<tr>
<td></td>
<td>./products/one/server/bloxtools/bloxtools_apache/conf/httpd_simple.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>./products/one/server/bloxtools/bloxtools_common-httpd.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>./products/one/server/tmpl-captive-portal-common-httpd.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>./products/one/server/tmpl-bloxtools-httpd.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>./products/one/server/tmpl-one-httpd.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>./products/tests/server/src/bin/harness/datasets/httpd-ibdelay.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>./webui/httpd.conf</td>
<td></td>
</tr>
<tr>
<td><strong>Apache</strong></td>
<td>A config maker, cipher suites are configurable via serial console</td>
<td><strong>OpenSSL C-functions</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td><code>/products/one/server/src/bin/make_httpd_conf/db.c</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>set_tls_protocols</code> --- will enable &quot;enable_tlsv1&quot;, &quot;enable_tlsv1_1&quot; and &quot;enable_tlsv1_2&quot;,&quot;ALL&quot; in db based on its param</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>set_tls_ciphers</code> --- validates &quot;cipher_suite&quot; param</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>/products/one/server/src/bin/serial_console/set.c</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>check_ssl_connection()</code> --- To check ssl connection</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>download_gm_certificate</code> --- Download certificate from GM</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>printf_certificate()</code> --- To print certificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>/products/one/server/src/bin/clusterd/util.c</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Functions <code>cd_start_replica_vpn</code>, <code>cd_start_master_vpn</code> run command <code>cd_start_replica_vpn</code> run command <code>cd_start_master_vpn</code> run command</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>/usr/sbin/openvpn</code> with arguments including:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>--ca /infoblox/security/keys/vpn_CaCerts.pem</code>,</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>--cert /infoblox/security/keys/node.crt</code>,</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>--key /infoblox/security/keys/node.key</code>,</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>--cipher AES-128-CB</code>,</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>--tls-cipher DHE-RSA-AES256-SHA</code>,</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>--auth SHA1</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>/products/one/server/src/bin/clusterd/sendmsg_handshake.c</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This module uses functions <code>cd_derive_serial</code>, <code>cd_sign_msg</code> from module</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>/products/one/server/src/bin/clusterd/util.c</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function <code>cd_derive_serial</code> derives a serial number from a string using SHA1 digest algorithm,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>it is used in function <code>cd_sendmsg_handshake_resp_req</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function <code>cd_sign_msg</code> signs a message with HMAC-SHA256,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>it is used in functions <code>cd_sendmsg_handshake_approval</code>,</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>cd_sendmsg_handshake_request_tunnel</code>,</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>cd_sendmsg_handshake_tunnel_approved</code>,</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>cd_sendmsg_handshake_new_master</code>, <code>cd_sendmsg_handshake_restart</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This module uses functions <code>ib_generate_authn_challenge</code>,</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ib_generate_authn_response</code>, <code>ib_generate_authn_response_2</code> from module</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>/common/server/src/lib/security/security_functions.c</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function <code>ib_generate_authn_challenge</code> generates auth challenge, it performs base64 encoding with OpenSSL function <code>EVP_EncodeBlock</code>,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>it is used in function <code>cd_sendmsg_handshake_challenge</code>,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function <code>ib_generate_authn_response</code> generates auth response computing MD5 hash, it is used in NIOS versions less than 6.3,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function <code>ib_generate_authn_response_2</code> generates auth response using HMAC_SHA256 algorithm, it is used in NIOS versions equal or greater than 6.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>they are used in function <code>cd_sendmsg_handshake_resp_req</code></td>
<td></td>
</tr>
</tbody>
</table>
This module uses functions `cd_derive_serial`, `cd_verify_msg` from module `/products/one/server/src/bin/clusterd/util.c`

Function `cd_derive_serial` derives a serial number from a string using SHA1 digest algorithm,

it is used in functions `cd_master_handshake_chal`,
`cd_potential_master_handshake_chal`, `cd_master_handshake_resp_chal`,
`cd_master_handshake_resp_req`, Function
`cd_potential_master_handshake_resp_req`, `cd_replica_handshake_resp_chal`

Function `cd_verify_msg` verifies a message signed by HMAC-SHA256,

it is used in functions `cd_master_handshake_approval_verify`,
`cd_master_handshake_tunnel_request_verify`,
`cd_potential_master_handshake_verify`,
`cd_master_handshake_new_master_verify`,
`cd_replica_handshake_approval`, `cd_replica_handshake_tunnel_approved`,
`cd_replica_handshake_restart`

This module uses functions `ib_generate_authn_challenge`,
`ib_generate_authn_response`, `ib_generate_authn_response_2` from module
`./common/server/src/lib/security/security_functions.c`

Function `ib_generate_authn_challenge` generates auth challenge, it performs base64 encoding with OpenSSL function `EVP_EncodeBlock`,

it is used in functions `cd_master_handshake_chal`,
`cd_potential_master_handshake_chal`

Function `ib_generate_authn_response` generates auth response computing MD5 hash, it is used in NIOS versions less than 6.3,

Function `ib_generate_authn_response_2` generates auth response using HMAC_SHA256 algorithm, it is used in NIOS versions equal or greater than 6.3,

they are used in functions `cd_master_handshake_chal`,
`cd_potential_master_handshake_chal`, `cd_master_handshake_resp_chal`,
`cd_master_handshake_resp_req`, `cd_potential_master_handshake_resp_req`,
`cd_replica_handshake_resp_chal`

To generate host keys

```
ssh-keygen -t rsa -f "$SSHD_HOST_RSA_KEY" >/dev/null
ssh-keygen -t dsa -f "$SSHD_HOST_DSA_KEY"
```

Remote authentication

Active Directory Services
`./products/one/server/src/pyabs/ad_auth.py`, imports ldap package
Function `AdAuthService.authenticate` does AD authentication,

it uses function `make_ldap_url(address, port, ssl)` from module
`./products/one/server/src/pyabs/ldap_auth_service.py`
to make up ldap url as ldaps://address:port if property 'encryption' = 'SSL'
otherwise the url prefix is ldap://,
the ldap url is used in function call 'conn = ldap.initialize(url)'

No OpenSSL function calls

Remote authentication

LDAP Services
`./products/one/server/src/pyabs/ldap_auth_service.py`, imports ldap package
Function `LdapAuthService.authenticate` authenticates users against LDAP servers,

it uses function `make_ldap_url(address, port, ssl)` from this module
to make up ldap url as ldaps://address:port if property 'encryption' = 'SSL'
otherwise the url prefix is ldap://,
the ldap url is used in function call 'conn = ldap.initialize(url)'

No OpenSSL function calls

Remote authentication

RADIUS Services
`./products/one/server/src/pyabs/radius_auth_service.py`

Function `RadiusAuthService.authenticate` does RADIUS authentication,

it uses functions from module
`./products/one/server/src/lib/one_rtxml_functions/radius.c`

No OpenSSL function calls
<table>
<thead>
<tr>
<th>Remote authentication</th>
<th>RADIUS Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>./products/one/server/src/lib/one_rtxml_functions/radius.c</td>
<td></td>
</tr>
<tr>
<td>Function radius_generate_acct_request_authenticator generates Accounting Request Authenticator (RequestAuth = MD5), it is used in this module, functions radius_accounting_start, admin_radius_accounting_test</td>
<td></td>
</tr>
<tr>
<td>Function radius_verify_message_authenticator recalculates the Message-Authenticator and compares with the received Message-Authenticator (MD5), it is used in this module, function radius_verify_response_packet</td>
<td></td>
</tr>
<tr>
<td>Function radius_verify_response_authenticator verifies the Received response authenticator (MD5),</td>
<td></td>
</tr>
<tr>
<td>Function radius_generate_message_authenticator generates a message authenticator (Message-Authenticator = HMAC-MD5),</td>
<td></td>
</tr>
<tr>
<td>Function radius_encrypt_user_password encrypts User-Password (MD5),</td>
<td></td>
</tr>
<tr>
<td>Function radius_encode_chap_password encodes CHAP-Password (MD5), they are used in this module, functions radius_access_request, radius_redo_access_request</td>
<td></td>
</tr>
<tr>
<td>OpenSSL C-functions:</td>
<td></td>
</tr>
<tr>
<td>MD5_Init, MD5_Update, MD5_Final used in radius_generate_acct_request_authenticator, radius_verify_response_authenticator, radius_encrypt_user_password, radius_encode_chap_password</td>
<td></td>
</tr>
<tr>
<td>HMAC_Init, HMAC_Update, HMAC_Final, HMAC_CTX_cleanup used in functions radius_generate_message_authenticator, radius_verify_message_authenticator</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remote authentication</th>
<th>RADIUS Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>./products/one/server/src/bin/admin_radius_acct/admin_radius_acct.c</td>
<td></td>
</tr>
<tr>
<td>Function radius_generate_acct_request_authenticator generates Accounting Request Authenticator (RequestAuth = MD5), it is used in this module, function radius_redo_accounting_request</td>
<td></td>
</tr>
<tr>
<td>Function radius_generate_acct_response_authenticator generates Accounting response authenticator (MD5), it is used in this module, function radius_acct_response_packet</td>
<td></td>
</tr>
<tr>
<td>Function radius_verify_acct_request_authenticator verifies the Received Acct request authenticator (MD5), it is used in this module, function radius_verify_request_packet</td>
<td></td>
</tr>
<tr>
<td>Function radius_verify_response_authenticator verifies the Received response authenticator (MD5),</td>
<td></td>
</tr>
<tr>
<td>Function radius_verify_message_authenticator recalculates the Message-Authenticator and compares with the received Message-Authenticator (HMAC-MD5), they are used in this module, function radius_verify_response_packet</td>
<td></td>
</tr>
<tr>
<td>OpenSSL C-functions:</td>
<td></td>
</tr>
<tr>
<td>MD5_Init, MD5_Update, MD5_Final used in radius_generate_acct_request_authenticator, radius_generate_acct_response_authenticator, radius_verify_acct_request_authenticator, radius_verify_response_authenticator</td>
<td></td>
</tr>
<tr>
<td>HMAC_Init, HMAC_Update, HMAC_Final, HMAC_CTX_cleanup used in function radius_verify_message_authenticator</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remote authentication</th>
<th>TACACS+ Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>./products/one/server/src/pyabs/tacacsplus_auth.py</td>
<td></td>
</tr>
<tr>
<td>Function TacacsplusAuthService.authenticate does TACACS+ authentication, it uses functions from modules: ./products/one/server/src/pyutil/tacacs.c ./products/one/server/src/lib/one_tacacs/tacacs.c which use functions from libtacplus.so</td>
<td></td>
</tr>
<tr>
<td>No OpenSSL function calls</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remote authentication</th>
<th>Certificate Authentication Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>./products/one/server/src/pyabs/ocsp_auth.py</td>
<td></td>
</tr>
<tr>
<td>Function OcspAuthService.authenticate does OCSP verification, it uses functions from module ./products/one/server/src/lib/one_ocsp/ocsp.c, see ocsp in this table</td>
<td></td>
</tr>
<tr>
<td>Function OcspAuthService.__get_responders_from_aia gets OCSP responder address(es) from aia, used in class function __get_effective_responders</td>
<td></td>
</tr>
<tr>
<td>Openssl command: openssl x509 -in cert_file -noout -ocsp_uri used in function OcspAuthService.__get_responders_from_aia</td>
<td></td>
</tr>
</tbody>
</table>
| **Secure syslog** | Config maker: ./products/one/server/src/pyabs/syslog_config.py
get_certificate_hash_from_fil | openssl -x509 -noout -hash -in "filename"

| **infoblox pki lib** | ./products/one/server/src/lib/pki/ipki_store.c | OpenSSL C-functions:
X509_digest with digest type=SHA512 used
function calculate_certificate_sha_512_fingerprint
X509_getIssuerName, X509_getSerialNumber,
X509_getSubjectName, X509_getPublicKey,
X509_free used in functions
convert_certificate_to_db
ipki_check_ca_cert_around_csrs,
ipki_find_csr_with_cert, X509_REQ_get_subject_name,
X509_REQ_getPublicKey, EVP_PKEY_bits,
X509_REQ_free used in function
convert_csr_buf_to_csr_db

| **infoblox pki lib** | ./products/one/server/src/lib/pki/ipki_api.c | OpenSSL C-functions:
X509_getSubjectName, X509_getPublicKey,
EVP_PKEY_bits, X509_get_notBefore,
X509_get_notAfter, X509_free used in functions
ipki_parse_cert_info,
ipki_parse_csr_info,
X509_REQ_getSubjectName,
X509_REQ_getPublicKey, EVP_PKEY_bits,
PEM_read_bio_X509_AUX, PEM_read_bio_X509,
X509_getSubjectName, X509_getIssuerName,
X509_getPublicKey, X509_checkCA,
EVP_PKEY_bits, X509_get_notBefore,
X509_get_notAfter used
in function ipki_get_cert_data,
PEM_read_bio_X509_REQ, X509_REQ_free used in
functions ipki_sign_csr_and_encode_cert,
ipki_sign_csr_by_ca

| **infoblox pki lib** | ./products/one/server/src/lib/pki/ipki_util.c | OpenSSL C-functions:
OpenSSL_add_all_ciphers, OpenSSL_add_all_digests,
ERR_load_crypto_strings used in function ipki_init
PEM_write_bio_X509, PEM_read_bio_X509,
X509_free used in function
ipki_parse_cert_info,
ipki parse_csr_info,
X509_REQ_getSubjectName,
X509_REQ_getPublicKey, EVP_PKEY_bits,
PEM_read_bio_X509_REQ, X509_REQ_free used in
functions ipki_sign_csr_and_encode_cert,
ipki_sign_csr_by_ca

Macro #define DEFAULT_KEY_CIPHER>>EVP_des_ede3_cbc(), it is used in function
ipki_key_bin_to_pem as an argument of call
PEM_write_bio_PrivateKey

Function ipki_init initializes openssl context,
it is used in modules:
OpenSSL_add_all_ciphers, OpenSSL_add_all_digests,
ERR_load_crypto_strings used in function ipki_init
PEM_write_bio_X509, PEM_read_bio_X509,
Function ipki_cert_bin_to_pem writes DER encoded cert to the given file in PEM format, it is used in modules:
/products/dns/server/src/bin/make_dtc_conf/make_healthd_conf.c, function mdc_healthd_certificates
/products/dns/server/src/bin/ciscoise_syncd/ciscoise_onedb.c, function _fill_srv_properties
/products/one/server/src/lib/one_rtxml_functions/system_administration.c, function one_export_any_cert
/products/one/server/src/pyutil/ibutil.c, function util_one_import_https_certificate
/products/one/server/src/bin/make_default_apache_cert/main.c, function mhc_write_default_https_cert_files

ipki_cert_bin_to_pem which is used in the following python modules:
/products/one/server/src/bin/make_syslog_conf/main.c, function msc_write_syslog_ng_conf
/products/one/server/src/bin/make_https_cert/main.c, function mhc_write_https_cert_files
/products/ifmap/server/src/bin/ifmapcd/client.c, function ifmap_get_config
/products/one/server/src/pyutil/ibutil.py, function
/products/one/server/src/pyabs/tae_ca_certificate.py, function TaeCACertificate._check_cert
/products/one/server/src/bin/util/make_certs.py, function make_cert_and_key
/products/ifmap/server/src/pyabs/ifmap_ca_certificate.py, function IfmapCACertificate._check_cert

Function ipki_cert_pem_to_bin - given a file that contains a PEM formatted cert, returns its DER encoded data, it is used in modules:
/products/one/server/src/lib/one_rtxml_functions/system_administration.c, functions one_import_ca_certificate, one_import_app_certificate, one_import_pkcs12
/products/one/server/src/pyutil/ibutil.c, function util_one_import_https_cert

Function ipki_key_bin_to_pem writes DER encoded private key to the given file in PEM format, PEM_write_bio_PrivateKey, PEM_read_bio_PrivateKey, EVP_PKEY_free used in functions ipki_key_
/ipki_key_pem_to_bin, one_import_https_cert
EVP_des_ede3_cbc used in macro DEFAULT_KEY_CIPHER

Function ipki_key_pem_to_bin, one_import_https_cert

Function ipki_key_bin_to_pem writes DER encoded private key to the given file in PEM format,
it is used in modules:
./products/one/server/src/pyutil/ibutil.c, function util_ipki_key_bin_to_pem
./products/one/server/src/bin/make_default_apache_cert/main.c, function
mhc_write_default_https_cert_files
./products/one/server/src/bin/makeHttpsCert/main.c, function
mhc_write_https_cert_files
./products/ifmap/server/src/bin/ifmapcd/client.c,
./ifmap/server/src/bin/ifmapcd/client.c, function ifmap_get_config
./products/one/server/src/pyutil/util.py, function ipki_key_bin_to_pem which is
used in the following python module:
./products/one/server/src/bin/make_certs.py, function make_cert_and_key
Function ipki_key_pem_to_bin - given a file that contains a PEM formatted
private key, returns its DER encoded data,
it is used in module:
./products/one/server/src/bin/make_default_apache_cert/main.c, function
mhc_read_https_cert_files

infoblox pki lib
./products/one/server/src/lib/pki/ipki_gen.c
Function ipki_set_serial_number sets a certificate serial number,
it is used in this module, functions ipki_create_selfsigned_cert, ipki_sign_cert
Function ipki_create_key creates a public/private key pair,
it is used in this module, function ipki_generate_csr
Function ipki_build_csr builds a CSR from given info,
it is used in this module, functions ipki_generate_csr, ipki_resign_csr
Function ipki_check_selfsigned_cert checks if a cert is self-signed,
it is used in module
./products/one/server/src/lib/one_rtxml_functions/system_administration.c,
function one_get_https_cert
Function ipki_create_selfsigned_cert generates a self signed cert,
it is used in modules:
./products/one/server/src/lib/pki/ipki_api.c, functions
ipki_generate_and_store_server_cert, ipki_sign_csr_and_encode_cert
./products/one/server/src/bin/make_default_apache_cert/main.c, function
mhc_write_default_https_cert_files
Function ipki_sign_cert signs a cert with a CA and returns the binary cert in a
buffer,
it is used in module ./products/one/server/src/lib/pki/ipki_api.c, function
ipki_sign_csr_by_ca

OpenSSL C-functions:
X509_get_pubkey, X509_get_subject_name
X509_get_issuer_name, X509_set_serialNumber
X509_free used in functions ipki_set_serial_number,
ipki_check_selfsigned_cert
EVP_PKEY_new, RSA_generate_key,
EVP_PKEY_assign_RSA, RSA_free used in
ipki_create_key,
X509_REQ_new, X509_REQ_sign (with SHA1/SHA256),
X509_REQ_free used in function ipki_build_csr,
X509_REQ_to_X509, X509_set_version,
X509_set_issuer_name, X509_sign (with SH
X509_free, X509_REQ_free used in function
ipki_create_selfsigned_cert, ipki_sign_cert

List of SSL ciphers in an OpenSSL format
./products/dns/server/src/pyabs/idns_util.py
openssl x509 -in "pem_path" -out "crt_path" -text
openssl pkey -in "pem_path” -out "key_path”
openssl pkey -in "pem_path” -out "key_path”
openssl rsa -nout -modulus -in "key_path”
openssl x509 -nout -modulus -in "crt_path”

DTC
https, sip monitors communication:
./products/dns/server/src/pyabs/idns_util.py
Function
add_idns_certificate()
DTC

Function
add_idns_certificate()

Certificates in PEM or PKCS#12 format associated with HTTP and SIP health monitors

```
openssl pkcs12 -in "cert_and_key_path" -info -noout -passin pass:
openssl pkcs12 -in "cert_and_key_path" -nodes -out "pem_path" -passin pass:
```

DTC

The below files doesn't have any crypthographic function

- ./products/dns/server/src/pyabs/idns_common.py
- ./products/dns/server/src/pyabs/idns_certificate.py
- ./products/dns/server/src/pyabs/idns_monitor_http.py
- ./products/dns/server/src/pyabs/idns_monitor_sip.py

Outbound3

Function:
WrapSSLSocket class is defined and called for WrapHTTPSCConnection.

A generate certificate button on DXL endpoint
Upload and validate DXL endpoint certificate

Outbound3

The above mentioned file doesn't exists now.

In the below files encryption algorithms are not used

- ./products/one/server/src/outbound/lib/records.py
- ./products/one/server/src/outbound/lib/service_manager.py
- ./products/one/server/src/outbound/lib/ssl_requests.py

A generate certificate button on DXL endpoint
Upload and validate DXL endpoint certificate

bind9

Function

Function openssldsa_createctx() creates, initializes and setup Digest context.
Function openssldsa_destroyctx() cleans up digest context ctx and frees up the space allocated to it.
Function openssldsa_adddata() hashes cnt data to digest context ctx.
Function openssldsa_sign()signs the data in ctx using the private key pkey and places the signature in sig.
Function openssldsa_verify() verifies the data
Function openssldsa_destroy() DSA_free() is called.
openssldsa_fromdns()
Function openssldsa_parse() is used to parse private key

OpenSSL C-functions

EVP_MD_CTX_create,EVP_DigestInit_ex,
EVP_MD_CTX_destroy,
EVP_DigestUpdate,EVP_PKEY_new,
EVP_PKEY_set1_DSA,EVP_PKEY_free,
EVP_DigestFinal_ex,DSA_SIG_new,
DSA_do_verify,DSA_SIG_free,DSA_free

bind9

Function ATF_TC_BODY() is used to generate OPENSSL_GOST private key

OpenSSL C-functions

EVP_PKEY_bits,EVP_PKEY_get0,
EC_KEY_set_private_key,
EC_KEY_get0_private_key,
pk11_get_session,pkcs_C_CreateObject,
pkcs_C_SignInit,pkcs_C_Sign
<table>
<thead>
<tr>
<th>Function Name</th>
<th>Description</th>
<th>OpenSSL C-functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>opensslrsa_createctx()</td>
<td>creates, initializes and setup Digest context based on algorithm</td>
<td>EVP_MD_CTX_create, EVP_md5, EVP_sha1, EVP_sha256, EVP_sha512, EVP_DigestInit_ex, EVP_MD_CTX_destory, EVP_MD_CTX_destroy, EVP_DigestUpdate, EVP_SignFinal, RSA_sign, EVP_PKEY_get1_RSA, RSA_free, RSA_size, RSA_public_decrypt, EVP_PKEY_set1_RSA, RSA_generate_key, EVP_PKEY_free, EVP_PKEY_get1_RSA, EVP_PKEY_new</td>
</tr>
<tr>
<td>opensslrsa_destroyctx()</td>
<td>cleans up digest context ctx and frees up the space allocated to it.</td>
<td></td>
</tr>
<tr>
<td>opensslrsa_adddata()</td>
<td>hashes cnt data to digest context ctx.</td>
<td></td>
</tr>
<tr>
<td>opensslrsa_sign()</td>
<td>signs the data in ctx using the private key pkey and places the signature in sig.</td>
<td></td>
</tr>
<tr>
<td>opensslrsa_verify()</td>
<td>verifies the data</td>
<td></td>
</tr>
<tr>
<td>opensslrsa_generate()</td>
<td>generates keys.</td>
<td></td>
</tr>
<tr>
<td>opensslrsa_isprivate()</td>
<td>RSA private key verified.</td>
<td></td>
</tr>
<tr>
<td>opensslrsa_destroy()</td>
<td>RSA_free() is called</td>
<td></td>
</tr>
<tr>
<td>opensslrsa_todns(), opensslrsa_fromdns(), opensslrsa_tofile(), opensslrsa_parse()</td>
<td>is used to parse private key</td>
<td></td>
</tr>
<tr>
<td>opensslrsa_fromlabel()</td>
<td>public key generation</td>
<td></td>
</tr>
<tr>
<td>openssldh_computesecret()</td>
<td>to generate secret key</td>
<td></td>
</tr>
<tr>
<td>openssldh_generate()</td>
<td>is used to generate DH key.</td>
<td></td>
</tr>
<tr>
<td>openssldh_destroy()</td>
<td>DH_free is called</td>
<td></td>
</tr>
<tr>
<td>openssldh_fromdns()</td>
<td></td>
<td></td>
</tr>
<tr>
<td>openssldh_parse()</td>
<td>is used to parse private key</td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_createctx_verify()</td>
<td>pk11_ctx object is verified with its algorithm mechanism</td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_destroyctx()</td>
<td>Destroys pkcs object.</td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_adddata()</td>
<td>sign/Data update to pkcs object</td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_sign()</td>
<td>pkcs_C_SignFinal() is called from here</td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_verify()</td>
<td>verify pk11_ctx</td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_compare()</td>
<td>comparing two keys passed to it.</td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_generate()</td>
<td>generate PKCS keypairs.</td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_isprivate()</td>
<td>get the attribute by type from it.</td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_destroy()</td>
<td>destroying key and its data from dst_key_t</td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_todns()</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_fromdns()</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_tofile()</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_fetch()</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsa_check()</td>
<td>check for private and public attributes in pk11 object.</td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_parse()</td>
<td>parsing public and private key</td>
<td></td>
</tr>
<tr>
<td>pkcs11rsa_fromlabel()</td>
<td>find the objects and its attribute values.</td>
<td></td>
</tr>
<tr>
<td>bind9</td>
<td>bind9/lib/dns/openssl_link.c</td>
<td>OpenSSL C-functions</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td>./bind9/lib/dns/openssl gost_link.c</td>
<td>EVP_gost, EVP_MD_CTX_init,</td>
</tr>
<tr>
<td></td>
<td>Function isc_gost_init() creates, initializes and setup Digest</td>
<td>EVP_DigestInit,</td>
</tr>
<tr>
<td></td>
<td>Function isc_gost_invalidate() cleanup of ctx</td>
<td>EVP_DigestFinal</td>
</tr>
<tr>
<td></td>
<td>Function isc_gost_update() does Digest update</td>
<td>EVP_MD_CTX_cleanup,</td>
</tr>
<tr>
<td></td>
<td>Function isc_gost_final() digest final</td>
<td>EVP_DigestUpdate,</td>
</tr>
<tr>
<td></td>
<td>Function opensslgost_createctx() creates, initializes and setup Digest</td>
<td>EVP_MD_CTX_create,</td>
</tr>
<tr>
<td></td>
<td>Function opensslgost_destroyctx() destroys the setup digest.</td>
<td>EVP_DigestInit_ex,</td>
</tr>
<tr>
<td></td>
<td>Function opensslgost_adddata() perform Digest update.</td>
<td>EVP_MD_CTX_destroy,</td>
</tr>
<tr>
<td></td>
<td>Function opensslgost_sign() sign the private key.</td>
<td>EVP_SignFinal,</td>
</tr>
<tr>
<td></td>
<td>Function opensslgost_compare() compares two keys</td>
<td>EVP_VerifyFinal,EVP_PKEY_cmp,</td>
</tr>
<tr>
<td></td>
<td>Function progress_cb() private key generation info.</td>
<td>EVP_PKEY_CTX_get_app_data,</td>
</tr>
<tr>
<td></td>
<td>Function opensslgost_generate() initialize and gost key generation</td>
<td>EVP_PKEY_CTX_get_keygen_info,</td>
</tr>
<tr>
<td></td>
<td>Function opensslgost_isprivate() get private key</td>
<td>EVP_PKEY_CTX_new_id,</td>
</tr>
<tr>
<td></td>
<td>Function opensslgost_destroy() free the private key</td>
<td>EVP_PKEY_CTX_set_cb,</td>
</tr>
<tr>
<td></td>
<td>Function opensslgost_tofile()</td>
<td>EVP_PKEY_CTX_set_app_data,</td>
</tr>
<tr>
<td></td>
<td>function opensslgost_parse() parsing public and private key</td>
<td>EVP_PKEY_keygen_init,</td>
</tr>
<tr>
<td></td>
<td>dst__openssl_destroy --- connection termination of openssl</td>
<td>EVP_PKEY_CTX_ctrl_str,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVP_PKEY_keygen,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVP_PKEY_get0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVP_PKEY_free, EC_KEY_get0_private_key,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EC_KEY_set_private_key,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EC_KEY_set_public_key, EVP_PKEY_free</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVP_cleanup</td>
</tr>
<tr>
<td>bind9</td>
<td>bind9/lib/dns/openssl_ecdsa_link.c</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function openssl_ecdsa_createctx() creates, initializes and setup Digest context.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function openssl_ecdsa_destroyctx() cleans up digest context ctx and frees up the space allocated to it.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function openssl_ecdsa_adddata() hashes cnt data to digest context ctx.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function openssl_ecdsa_sign() signs the data in ctx using the private key pkey and places the signature in sig.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function openssl_ecdsa_verify() verifies the data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function openssl_ecdsa_compare() compares the keys</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function openssl_ecdsa_generate() generates ecdsa key</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function openssl_ecdsa_isprivate() get ecdsa private key</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function openssl_ecdsa_todns()</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function openssl_ecdsa_fromdns()</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function openssl_ecdsa_tofile()</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function ecdsa_check() check for the public key</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function openssl_ecdsa_parse() is used to parse private key</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OpenSSL C-functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVP_MD_CTX_create, EVP_sha256,</td>
</tr>
<tr>
<td>EVP_sha384, EVP_DigestInit_ex, EVP_MD_CTX_destroy,</td>
</tr>
<tr>
<td>EVP_DigestUpdate,</td>
</tr>
<tr>
<td>EVP_PKEY_get1_EC_KEY, EVP_DigestFinal,</td>
</tr>
<tr>
<td>ECDSA_do_sign, ECDSA_SIG_free</td>
</tr>
<tr>
<td>EC_KEY_free,</td>
</tr>
<tr>
<td>EVP_PKEY_get1_EC_KEY, EVP_DigestFinal,</td>
</tr>
<tr>
<td>ECDSA_SIG_new, ECDSA_do_verify,</td>
</tr>
<tr>
<td>EVP_PKEY_get1_EC_KEY, EVP_PKEY_cmp</td>
</tr>
<tr>
<td>EC_KEY_get0_private_key,</td>
</tr>
<tr>
<td>EC_KEY_new_by_curve_name,</td>
</tr>
<tr>
<td>EC_KEY_generate_key,</td>
</tr>
<tr>
<td>EVP_PKEY_new,</td>
</tr>
<tr>
<td>EVP_PKEY_set1_EC_KEY,</td>
</tr>
<tr>
<td>EVP_PKEY_free, EC_KEY_free,</td>
</tr>
<tr>
<td>EC_KEY_check_key,</td>
</tr>
<tr>
<td>EVP_PKEY_new,</td>
</tr>
<tr>
<td>EC_KEY_set_public_key,</td>
</tr>
<tr>
<td>EC_KEY_check_key,</td>
</tr>
<tr>
<td>EC_KEY_set_private_key</td>
</tr>
<tr>
<td>bind9</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>Function isc_sha224_init() -- Context is initialised to EVP_sha224</td>
</tr>
<tr>
<td>Function isc_sha224_invalidate() -- cleans up the context.</td>
</tr>
<tr>
<td>Function isc_sha224_update -- calls EVP_DigestUpdate()</td>
</tr>
<tr>
<td>Function isc_sha224_final -- checks for the context with digest</td>
</tr>
<tr>
<td>Function isc_sha256_init -- Context is initialised to EVP_sha224</td>
</tr>
<tr>
<td>Function isc_sha256_invalidate -- cleans up the context.</td>
</tr>
<tr>
<td>Function isc_sha256_update -- calls EVP_DigestUpdate()</td>
</tr>
<tr>
<td>Function isc_sha256_final -- checks for the context with digest</td>
</tr>
<tr>
<td>Function isc_sha512_init -- Context is initialised to EVP_sha224</td>
</tr>
<tr>
<td>Function isc_sha512_invalidate -- cleans up the context.</td>
</tr>
<tr>
<td>Function isc_sha512_update -- calls EVP_DigestUpdate()</td>
</tr>
<tr>
<td>Function isc_sha512_final -- checks for the context with digest</td>
</tr>
<tr>
<td>Function isc_sha384_init -- Context is initialised to EVP_sha224</td>
</tr>
<tr>
<td>Function isc_sha384_invalidate -- cleans up the context.</td>
</tr>
<tr>
<td>Function isc_sha384_update -- calls EVP_DigestUpdate()</td>
</tr>
<tr>
<td>Function isc_sha384_final -- checks for the context with digest</td>
</tr>
<tr>
<td>Function isc_sha224_end -- Converts the digest to readable format and cleans up</td>
</tr>
<tr>
<td>Function isc_sha256_end -- Converts the digest to readable format and cleans up</td>
</tr>
<tr>
<td>Function isc_sha512_end -- Converts the digest to readable format and cleans up</td>
</tr>
<tr>
<td>Function isc_sha384_end -- Converts the digest to readable format and cleans up</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>bind9</th>
<th>/bind9/lib/isc/hmacmd5.c</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function isc_hmacmd5_init -- Initialize the context to HMAC</td>
<td></td>
</tr>
<tr>
<td>Function isc_hmacmd5_invalidate -- clean up the context</td>
<td></td>
</tr>
<tr>
<td>Function isc_hmacmd5_update -- update the context with buffer.</td>
<td></td>
</tr>
<tr>
<td>Function isc_hmacmd5_sign -- To verify the sign</td>
<td></td>
</tr>
</tbody>
</table>

**OpenSSL C-functions**

- EVP_DigestInit
- EVP_MD_CTX_cleanup
- EVP_DigestUpdate
- EVP_DigestFinal

- HMAC_Init, EVP_md5
- HMAC_CTX_cleanup
- HMAC_Update, HMAC_Final
- pkcs_C_CreateObject
- pkcs_C_SignInit, pkcs_C_SignFinal
- pkcs_C_DestroyObject
- pkcs_C_SignUpdate, pkcs_C_DigestInit
- pkcs_C_DIGESTUpdate
- pkcs_C_DigestFinal
<table>
<thead>
<tr>
<th>bind9</th>
<th>./bind9/lib/isc/sha1.c</th>
<th>OpenSSL C-functions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Function isc_sha1_init -- context is initialised to EVP_sha1</td>
<td>EVP_DigestInit, EVP_MD_CTX_cleanup,</td>
</tr>
<tr>
<td></td>
<td>Function isc_sha1_invalidate -- clean up the context</td>
<td>EVP_DigestFinal</td>
</tr>
<tr>
<td></td>
<td>Function isc_sha1_update -- calls EVP_DigestUpdate</td>
<td>pkcs_C_DigestInit, pkcs_C_DigestFinal,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pkcs_C_DigestFinal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pkcs_C_DigestFinal, pkcs_C_DigestFinal,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pkcs_C_D DigestUpdate</td>
</tr>
<tr>
<td>bind9</td>
<td>./bind9/lib/isc/md5.c</td>
<td>OpenSSL C-functions</td>
</tr>
<tr>
<td></td>
<td>Function isc_md5_init -- context is initialised to EVP_md5</td>
<td>EVP_DigestInit, EVP_MD_CTX_cleanup,</td>
</tr>
<tr>
<td></td>
<td>Function isc_md5_invalidate -- clean up the context</td>
<td>EVP_DigestUpdate,</td>
</tr>
<tr>
<td></td>
<td>Function isc_md5_update -- calls EVP_DigestUpdate</td>
<td>EVP_MD_CTX_cleanup</td>
</tr>
<tr>
<td></td>
<td>Function isc_md5_final -- calls EVP_DigestFinal</td>
<td></td>
</tr>
<tr>
<td>bind9</td>
<td>./bind9/lib/isc/hmacsha.c</td>
<td>OpenSSL C-functions</td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha1_init -- context is initialised to EVP_sha1</td>
<td>HMAC_Init, HMAC_CTX_cleanup,</td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha1_invalidate -- clean up the context</td>
<td>HMAC_Update,</td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha1_update -- calls HMAC_Update</td>
<td>HMAC_Final,</td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha1_sign -- Check for the digest signature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha224_init -- context is initialised to EVP_sha224</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha224_invalidate -- clean up the context</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha224_update -- calls HMAC_Update</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha224_sign -- Check for the digest signature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha256_init -- context is initialised to EVP_sha256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha256_invalidate -- clean up the context</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha256_update -- calls HMAC_Update</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha256_sign -- Check for the digest signature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha384_init -- context is initialised to EVP_sha384</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha384_invalidate -- clean up the context</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha384_update -- calls HMAC_Update</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha384_sign -- Check for the digest signature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha512_init -- context is initialised to EVP_sha512</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha512_invalidate -- clean up the context</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha512_update -- calls HMAC_Update</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_hmacsha512_sign -- Check for the digest signature</td>
<td></td>
</tr>
<tr>
<td>bind9</td>
<td>./bind9/lib/isc/aes.c</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_aes128_crypt -- encrypts the data with EVP_aes_128_ecb</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_aes192_crypt -- encrypts the data with EVP_aes_192_ecb</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_aes256_crypt -- encrypts the data with EVP_aes_256_ecb</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function isc_aes_crypt -- encrypts the data in pkcs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OpenSSL C-functions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EVP_CIPHER_CTX_init,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EVP_EncryptInit,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EVP_CIPHER_CTX_set_padding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EVP_EncryptUpdate,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EVP_CIPHER_CTX_cleanup,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AES_set_encrypt_key,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AES_encrypt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pkcs_C_CreateObject,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pkcs_C_EncryptInit,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pkcs_C_Encrypt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pkcs_C_DestroyObject</td>
<td></td>
</tr>
<tr>
<td>bind9</td>
<td>./bind9/configure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OpenSSL C-functions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HMAC_Init,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HMAC_Update,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HMAC_Final</td>
<td></td>
</tr>
<tr>
<td>bind9</td>
<td>./bind9/config.h.win32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Below are the literal constants</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HAVE_EVP_SHA384,HAVE_EVP_SHA256,HAVE_EVP_SHA512,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HAVE_OPENSSL_DSA,HAVE_OPENSSL_ECDSA,HAVE_OPENSSL_GOST</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HAVE_PKCS11_ECDSA,HAVE_PKCS11_GOST,PREFER_GOSTASN1,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HAVE_OPENSSL_EVP_AES,HAVE_OPENSSL_AES,HMAC_RETURN_INT,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AES_SIT,HMAC_SHA1_SIT,HMAC_SHA256_SIT,HAVE_READLINE,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HAVE_GEOIP,HAVE_GEOIP_CITY_V6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OpenSSL C-functions</td>
<td></td>
</tr>
<tr>
<td>bind9</td>
<td>./bind9/bin/pkcs11/pkcs11-keygen.c</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Function main()</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OpenSSL C-functions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pkcs_C_GetMechanismInfo,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pk11_set_lib_name,pk11_get_session,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pkcs_C_GenerateKey,pkcs_C_GetAttribute,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pkcs_C_GenerateKeyPair,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pkcs_C_DestroyObject,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pkcs_C_FindObjectsFinal,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pk11_return_session</td>
<td></td>
</tr>
<tr>
<td>bind9</td>
<td>/bind9/bin/pkcs11/openssl-1.0.1j-patch</td>
<td>OpenSSL C-functions</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_active_delete,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_destroy_object,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_destroy_rsa_key_objects</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_destroy_dsa_key_objects,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_destroy_dh_key_objects,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_free_session_list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_library_init,OPENSSL_assert,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OPENSSL_free,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_destroy_rsa_object_priv</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_cipher_final,pk11_digest_final,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_find_digests,pk11_get_digest,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_active_remove,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_active_delete,pk11_DH_generate_key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_free_active_list,pk11_token_login,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RSA_get_ex_new_index,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RSA_set_ex_data,PEM_read_PrivateKey,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVP_PKEY_get1_RSA,EVP_PKEY_free,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RSA_free,EVP_PKEY_new,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVP_PKEY_assign_RSA,RSA_free</td>
</tr>
<tr>
<td>bind9</td>
<td>./bind9/bin/pkcs11/openssl-1.0.0o-patch</td>
<td>OpenSSL C-functions</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>bind9</td>
<td>pk11_have_dsa, pk11_destroy_dsa_object_pub,</td>
</tr>
<tr>
<td></td>
<td>bin/pkcs11/openssl-1.0.0o-patch</td>
<td>pk11_destroy_dsa_object_priv,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_destroy_dh_object,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_digest_final,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_destroy_cipher_key_objects,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_RSA_verify,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_RSA_private_encrypt,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_RSA_private_decrypt,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_RSA_init, pk11_RSA_finish,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_RSA_sign, pk11_RSA_verify,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_load_privkey, pk11_RSA_public_encrypt,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_RSA_private_encrypt_low,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_RSA_public_decrypt_low,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_RSA_private_decrypt_low,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>check_new_rsa_key_pub,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>check_new_rsa_key_priv,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_DSA_init, pk11_DSA_finish,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_dsa_do_sign,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_dsa_do_verify, check_new_dsa_key_priv,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_DH_init, pk11_DH_finish,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_DH_generate_key,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_DH_compute_key, pk11_active_add,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_active_find,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_RSA_private_encrypt_low,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_destroy_rsa_object_priv,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVP_PKEY_get1_RSA,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVP_PKEY_assign_RSA,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PEM_read_PrivateKey, EVP_PKEY_new,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVP_PKEY_assign_RSA, DSA_SIG_new,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pk11_destroy_dh_object,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVP_PKEY_assign_RSA,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EVP_PKEY_get1_RSA</td>
</tr>
</tbody>
</table>
| bind9 | .bind9/bin/pkcs11/openssl-0.9.8zc-patch | OpenSSL C-functions
| pk11_destroy_object,
| pk11_get_symmetric_cipher,
| pk11_find_digests,
| pk11_get_digest,
| pk11_active_add,pk11_active_find,
| RSA_padding_add_PKCS1_type_1,
| RSA_padding_add_none,
| pk11_RSA_private_encrypt_low,
| RSA_padding_check_PKCS1_type_1,
| RSA_padding_check_none,
| RSA_free,EVP_PKEY_free,
| pk11_DSA_init,pk11_DSA_finish,
| pk11_dsa_do_sign,DSA_SIG_new,
| pk11_finish,pk11_destroy,pk11_ctrl,
| PEM_read_PrivateKey |
| bind9 | .bind9/bin/tests/system/rsabigexponent/bigkey.c | OpenSSL C-functions
| Function
| main() |
| The below files dont have any cryptographic functions involved.
| .bind9/lib/dns/dst_openssl.h
| .bind9/lib/dns/tests/dh_test.c
| .bind9/lib/dns/dst_internal.h
| .bind9/lib/dns/dst_parse.c
| .bind9/lib/dns/dst_parse.h
| .bind9/lib/dns/dst_gost.h
| .bind9/config.h.in
| .bind9/lib/bind9/check.c
| .bind9/configure.in
| .bind9/lib/isc/include/pkcs11/pkcs11.h
| .bind9/lib/isc/include/isc/sha2.h
| .bind9/lib/isc/include/isc/hmacsha.h
| .bind9/lib/isc/include/isc/md5.h
| .bind9/lib/isc/include/isc/sha1.h
| .bind9/lib/isc/include/isc/hmacmd5.h
| .bind9/lib/dns/resolver.c
| .bind9/win32utils/Configure --- only configuration related doesnt have algorithms
| .bind9/bin/named/client.c
| .bind9/bin/named/server.c
| .bind9/bin/tools/isc-hmac-fixup.c
<p>| .bind9/bin/tests/hashes/t_hashes.c | OpenSSL C-functions |</p>
<table>
<thead>
<tr>
<th>unbound</th>
<th>./unbound/testcode/streamtcp.c</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>write_q() -- write a query over the TCP fd</td>
</tr>
<tr>
<td></td>
<td>recv_one() -- receive DNS datagram over TCP and print it</td>
</tr>
<tr>
<td></td>
<td>send_em() -- send the TCP queries</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>unbound</th>
<th>./unbound/testcode/unitmain.c</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>unbound</th>
<th>./unbound/testcode/petal.c</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>read_ssl_line -- Read one line from SSL</td>
</tr>
<tr>
<td></td>
<td>setup_ctx -- setup SSL context</td>
</tr>
<tr>
<td></td>
<td>setup_ssl -- setup SSL connection to the client</td>
</tr>
<tr>
<td></td>
<td>provide_file_10 -- provide file in transfer</td>
</tr>
<tr>
<td></td>
<td>provide_file_chunked --</td>
</tr>
<tr>
<td></td>
<td>do_service -- provide ssl service</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>unbound</th>
<th>./unbound/../../../../configure.ac load_gost_id()</th>
</tr>
</thead>
</table>
| unbound | /unbound/configure load_gost_id() | OpenSSL C-functions (names begin with CRYPTO_, TLSv1_, SSLv23_, SSL_CTX_, X509_, PEM_, EVP_, HMAC_, DH_, DSA_, RSA_)  
| unbound | /unbound/smallapp/unbound-anchor.c | PEM_read_bio_X509, PEM_read_X509, BIO_new_mem_buf, BIO_free  
|         | read_cert_bio()---read certificates from a PEM | SSL_CTX_new, SSL_new, SSL_set_connect_state, SSL_free, BIO_get_mem_data  
|         | read_cert_file---read the certificate file | write_ssl_line, BIO_reset, BIO_write, SSL_write, X509_get_ext_d2i, PKCS7_get0_signers, X509_get_subject_name, X509_NAME_get_text_by_NID, BIO_SEEK  
|         | read_builtin_cert --- read certificates from the builtin certificate | X509_STORE_set1_param, d2i_PKCS7_bio, PKCS7_verify, X509V3_EXT_print_fp, SSL_set_mode, SSL_set_fd, SSL_do_handshake, SSL_get_error, BIO_read, SSL_get_error, BIO_new_mem_buf, TLS_initiate, SSL_CTX_, X509_, PEM_, EVP_, HMAC_, DH_, DSA_, RSA_, PKCS7_get0_signers  
|         | read_cert_or_builtin --- read update cert file or use builtin | BIO_get_mem_data, SSL_ctx_set_state, SSL_CTX_free, BIO_seek, BIO_get_mem_data, SSL_get_peer_certificate, X509_free  
|         | setup_sslctx --- create SSL context |  
|         | TLS_initiate ---initiate TLS on a connection |  
|         | TLS_shutdown ---perform neat TLS shutdown |  
|         | write_ssl_line--- write a line over SSL |  
|         | read_ssl_line --- Read one line from SSL |  
|         | read_data_chunk--- Read chunk data |  
|         | do_chunked_read ---read chunked data from connection |  
|         | write_http_get-- transaction on SSL |  
|         | read_http_result --- read HTTP result from SSL |  
|         | do_chunked_zero_terminate ---read chunked data and zero terminate |  
|         | write_root_anchor --- write root anchor file |  
|         | verify_and_update_anchor --- Perform the verification and update of the trustanchor |  
|         | xml_charhandle ---XML handle character data |  
|         | handle_keydigest ---XML handle the KeyDigest start |  
|         | xml_is_zone_name --See if XML element equals the zone name |  
|         | xml_append_bio ---Append bio to bio |  
|         | xml_append_ds --- write the parsed xml-DS |  
|         | xml_parse_setup --- XML parser setup of the callbacks |  
|         | xml_parse ---Perform XML parsing of the root-anchors file |  
|         | get_usage_of_ex ---get key usage out of its extension |  
|         | get_valid_signers ---get valid signers from the list of signers |  
|         | verify_p7sig --- verify a PKCS7 signature |  
|         | write_root_anchor --- write root anchor file |  
|         | verify_and_update_anchor --- Perform the verification and update of the trustanchor |  

Copyright ©2019, Infoblox, Inc. All right reserved.
<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>OpenSSL C-functions (names begin with CRYPTO_, TLSv1_, SSLv23_, SSL_CTX_, X509_, PEM_, EVP_, HMAC_, DH_, DSA_, RSA_)</th>
</tr>
</thead>
<tbody>
<tr>
<td>setup_ctx()</td>
<td>setup SSL on the connection</td>
<td>SSL_CTX_new, SSL_CTX_set_options, SSL_CTX_use_PrivateKey_file, SSL_CTX_check_private_key, SSL_CTX_load_verify_locations, SSL_set_connect_state, SSL_set_mode, SSL_set_fd, SSL_do_handshake, setup_ssl, SSL_free, SSL_library_init, SSL_get_error, SSL_get_verify_result, SSL_get_peer_certificate, SSL_write, X509_free, SSL_CTX_set_verify</td>
</tr>
<tr>
<td>setup_ssl</td>
<td>setup SSL on the connection</td>
<td></td>
</tr>
<tr>
<td>send_file</td>
<td>send stdin to server</td>
<td></td>
</tr>
<tr>
<td>go_cmd</td>
<td>send command and display result</td>
<td></td>
</tr>
<tr>
<td>go</td>
<td>read config</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>OpenSSL C-functions (names begin with CRYPTO_, TLSv1_, SSLv23_, X509_, PEM_, EVP_, HMAC_, DH_, DSA_, RSA_)</th>
</tr>
</thead>
<tbody>
<tr>
<td>libworker_delete_env</td>
<td>delete libworker env</td>
<td>EVP_PKEY_asn1_find_str, EVP_PKEY_asn1_get0_info, EC_KEY_new_by_curve_name, o2i_ECPublicKey, EC_KEY_free, EVP_PKEY_new, EVP_PKEY_assign_EC_KEY, EVP_PKEY_free, EVP_MD_CTX_create, EVP_DigestInit_ex, EVP_DigestUpdate, EVP_DigestFinal_ex, EVP_MD_CTX_destroy</td>
</tr>
<tr>
<td>libworker_setup</td>
<td>setup fresh libworker struct</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>OpenSSL C-functions (names begin with CRYPTO_, TLSv1_, SSLv23_, X509_, PEM_, EVP_, HMAC_, DH_, DSA_, RSA_)</th>
</tr>
</thead>
<tbody>
<tr>
<td>sldns_key_EVP_load_gost_id()</td>
<td>store GOST engine reference loaded into OpenSSL library</td>
<td></td>
</tr>
<tr>
<td>sldns_ecdsa2pkey_raw()</td>
<td>ECDSA Key</td>
<td></td>
</tr>
<tr>
<td>sldns_digest EVP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>OpenSSL C-functions (names begin with CRYPTO_, TLSv1_, SSLv23_, X509_, PEM_, EVP_, HMAC_, DH_, DSA_, RSA_)</th>
</tr>
</thead>
<tbody>
<tr>
<td>daemon_delete()</td>
<td>Freeing the daemon process resource</td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>daemon_remote_create</td>
<td>Create a remote daemon</td>
<td></td>
</tr>
<tr>
<td>daemon_remote_delete</td>
<td>Delete a remote daemon</td>
<td></td>
</tr>
<tr>
<td>remote_accept_callback</td>
<td>Remote call back</td>
<td></td>
</tr>
<tr>
<td>clean_point</td>
<td>Decrease active count</td>
<td></td>
</tr>
<tr>
<td>ssl_print_text</td>
<td>Print SSL text</td>
<td></td>
</tr>
<tr>
<td>ssl_printf</td>
<td>Print style printing to the SSL connection</td>
<td></td>
</tr>
<tr>
<td>ssl_read_line</td>
<td>Read line from SSL connection</td>
<td></td>
</tr>
<tr>
<td>doverbosity</td>
<td>Do the verbosity of command</td>
<td></td>
</tr>
<tr>
<td>print_stats</td>
<td>Statistics info</td>
<td></td>
</tr>
<tr>
<td>print_longnum</td>
<td>Print the long num</td>
<td></td>
</tr>
<tr>
<td>printuptime</td>
<td>Print uptime stats</td>
<td></td>
</tr>
<tr>
<td>print_ext</td>
<td>Print extended stats</td>
<td></td>
</tr>
<tr>
<td>parse_arg_name</td>
<td>Parse commandline argument domain name</td>
<td></td>
</tr>
<tr>
<td>find_arg2</td>
<td>Find second argument</td>
<td></td>
</tr>
<tr>
<td>do_flush_zone</td>
<td>Remove all rrsets and keys from zone</td>
<td></td>
</tr>
<tr>
<td>do_flush_bogus</td>
<td>Remove all bogus rrsets</td>
<td></td>
</tr>
<tr>
<td>do_flush_negative</td>
<td>Remove all negative(NODATA, NXDOMAIN)</td>
<td></td>
</tr>
<tr>
<td>ssl_print_name_dp</td>
<td>Printout a delegation point info</td>
<td></td>
</tr>
<tr>
<td>print_root_fwds</td>
<td>Print root forwards</td>
<td></td>
</tr>
<tr>
<td>parse_delegpt</td>
<td>Parse args into delegpt</td>
<td></td>
</tr>
<tr>
<td>do_forward</td>
<td>Do the status command</td>
<td></td>
</tr>
<tr>
<td>parse_fs_args</td>
<td>Pass the arguments</td>
<td></td>
</tr>
<tr>
<td>do_dump_requestlist</td>
<td>Do the dump_requestlist</td>
<td></td>
</tr>
<tr>
<td>dump_infra_host</td>
<td>Callback for every host element</td>
<td></td>
</tr>
<tr>
<td>remote_get_opt_ssl</td>
<td>Routine to printout option values over SSL</td>
<td></td>
</tr>
<tr>
<td>do_get_option</td>
<td>Do the get_option command</td>
<td></td>
</tr>
<tr>
<td>do_list_forwards</td>
<td>Do the list_forwards command</td>
<td></td>
</tr>
<tr>
<td>do_list_local_zones</td>
<td>Do the list_local_zones</td>
<td></td>
</tr>
<tr>
<td>handle_req</td>
<td>Handle remote control request</td>
<td></td>
</tr>
</tbody>
</table>

OpenSSL C-functions (names begin with CRYPTO_, TLSv1_, SSLv23_, SSL_CTX_, X509_, PEM_, EVP_, HMAC_, DH_, DSA_, RSA_)
- SSL_CTX_new
- SSL_CTX_set_options
- SSL_CTX_use_certificate_file
- SSL_CTX_use_PrivateKey_file
- SSL_CTX_check_private_key
- SSL_CTX_load_verify_locations
- SSL_CTX_set_client_CA_list
- SSL_CTX_set_verify
- SSL_CTX_free
- SSL_new
- SSL_set_accept_state
- SSL_free
- SSL_shutdown
- SSL_write
- SSL_get_error
- SSL_set_mode
- SSL_set_fd
- X509_free
- SSL_setbaby
- SSL_set_verify
- SSL_get_verify_result
- SSL_get_peer_certificate
- X509_free
<table>
<thead>
<tr>
<th>unbound</th>
<th>./unbound/validator/val_secalgo.c</th>
</tr>
</thead>
<tbody>
<tr>
<td>ds_digest_size_supported -- Return size of DS digest according to its hash algorithm</td>
<td></td>
</tr>
<tr>
<td>do_gost94 -- Perform GOST hash</td>
<td></td>
</tr>
<tr>
<td>secalgo_ds_digest</td>
<td></td>
</tr>
<tr>
<td>setup_dsa_sig -- Setup DSA key digest in DER encoding</td>
<td></td>
</tr>
<tr>
<td>setup_ecdsa_sig -- Setup the ECDSA signature</td>
<td></td>
</tr>
<tr>
<td>setup_key_digest -- Setup key and digest for verification</td>
<td></td>
</tr>
<tr>
<td>verify_canonrrset -- Check a canonical sig+rrset</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OpenSSL C-functions (names begin with CRYPTO_, TLSv1_, SSLv23_, SSL_CTX_, X509_, PEM_, EVP_, HMAC_, DH_, DSA_, RSA_)</td>
</tr>
<tr>
<td></td>
<td>SHA_DIGEST_LENGTH, SHA256_DIGEST_LENGTH, EVP_get_digestbyname, sldns_digest EVP,SHA1,SHA256, do_gost94,SHA384</td>
</tr>
<tr>
<td></td>
<td>SHA384_DIGEST_LENGTH,DSA_SIG_new, i2d_DSA_SIG,EVP_PKEY_new</td>
</tr>
<tr>
<td></td>
<td>DSA_SIG_free,ECDSA_SIG_new,i2d_ECDSA_SIG,EVP_PKEY_assign_RSA, EVP_sha256,EVP_sha512, EVP_sha1,EVP_sha256,EVP_sha384, EVP_PKEY_free,EVP_MD_CTX_init, EVP_VerifyInit, EVP_PKEY_free, EVP_VerifyUpdate,EVP_VerifyFinal, EVP_MD_CTX_cleanup,PK11_Verify,</td>
</tr>
<tr>
<td>unbound</td>
<td>./unbound/util/alloc.c unbound_lite_i2d_DSA_SIG</td>
</tr>
<tr>
<td></td>
<td>OpenSSL C-functions (names begin with CRYPTO_, TLSv1_, SSLv23_, SSL_CTX_, X509_, PEM_, EVP_, HMAC_, DH_, DSA_, RSA_)</td>
</tr>
<tr>
<td></td>
<td>i2d_DSA_SIG</td>
</tr>
<tr>
<td>unbound</td>
<td>./unbound/util/net_help.c</td>
</tr>
<tr>
<td></td>
<td>listen_sslctx_create ---creates sslctx</td>
</tr>
<tr>
<td></td>
<td>connect_sslctx_create-- connect ssl</td>
</tr>
<tr>
<td></td>
<td>outgoing_ssl_fd--- outgoing ssl descriptor</td>
</tr>
<tr>
<td></td>
<td>OpenSSL C-functions (names begin with CRYPTO_, TLSv1_, SSLv23_, SSL_CTX_, X509_, PEM_, EVP_, HMAC_, DH_, DSA_, RSA_)</td>
</tr>
</tbody>
</table>
| | SSL_CTX_new,SSL_CTX_set_options, SSL_CTX_use_certificate_file, SSL_CTX_free,SSL_CTX_set_client_CA_list, SSL_CTX_get_verify_locations,SSL_CTX_set_stream再也 },SSL_CTX_set_verify,SSL_CTX_use_certificate_file, SSL_CTX_load_verify_locations,SSL_CTX_set_session_id,SSL_CTX_load_verify_locations,SSL_set_accept_state,SSL_set_cipher,SSL_set_cipher_list,SSL_set_mode,SSL_
| unbound                              | **Below files doesn't have encryption algorithms**  
|-------------------------------------|--------------------------------------------------  
| ./unbound/util/alloc.h               |                                                   
| ./unbound/config.h.in                |                                                   
| ./unbound/libunbound/unbound.h       |                                                   
| ./unbound/ldns/keyraw.h              | --No calls                                        
| ./unbound/libunbound/unbound.h       |                                                   
| ./unbound/doc/libunbound.3.in        |                                                   
| ./unbound/doc/Changelog              | --This contains few patches to openssl but not   
|                                     | related to crypthography functions.               
| ./unbound/acx_nintellabs.m4          | --Only function declaration related to HMAC       
|                                     |                                                   
| common                              | **OpenSSL C-functions (names begin with**         
|                                     | CRYPTO_, TLSv1_., SSLv23_., SSL_CTX_,           
|                                     | X509_, PEM_, EVP_, HMAC_, DH_, DSA_,            
|                                     |                                                   
|                                     | **OpenSSL C-functions:**                          
|                                     | Symmernic cryptography functions:                 
|                                     | EVP_BytesToKey, EVP_des_ede3_cbc,               
|                                     | EVP_sha1 used in function generateDESKey         
|                                     | EVP_aes_128_cbc, EVP_des_ede3_cbc                
|                                     | used in functions ib_encrypt_with_fixed_key,    
|                                     | ib_decrypt_with_fixed_key                        
|                                     | EVP_CIPHER_CTX_init,                             
|                                     | EVP_CIPHER_CTX_cleanup,                          
|                                     | EVP_DecryptInit[ex], EVP_DecryptUpdate,         
|                                     | EVP_DecryptFinal[ex]                            
|                                     | used in functions ibDecrypt,                     
|                                     | decrypt_with_fixed_key                           
|                                     | EVP_CIPHER_CTX_init,                             
|                                     | EVP_CIPHER_CTX_cleanup,                          
|                                     | EVP_EncryptInit[ex], EVP_EncryptUpdate,         
|                                     | EVP_EncryptFinal[ex]                            
|                                     | used in functions ibEncrypt,                     
|                                     | encrypt_with_fixed_key                           
|                                     | EVP_EncodeBlock used in functions                
|                                     | isecurity_base64_encode, isecurity_base64_encode 
|                                     | isecurity_base64_encode_raw                     
|                                     | isecurity_base64_decode, isecurity_base64_decode 
|                                     | MD5_Init, MD5_Update, MD5_Final                  
|                                     | Hmac and hash functions:                         
|                                     | SHA1_Init, SHA1_Update,                         
|                                     | SHA1_Final used in function                      
|                                     | ib_bin_SHAHash                                  
|                                     | HMAC, EVP_sha256 used in function                
|                                     | ib_bin_sha256hmac                               
|                                     | MD5_Init, MD5_Update, MD5_Final                  
|                                     | used in function ib_bin_md5Hash                 
|                                     | MD4_Init, MD4_Update, MD4_Final                  |
Function `ib_encrypt_with_fixed_key` implements the fixed key encryption using EVP_aes_128_cbc or EVP_des_ede3_cbc ciphers, calls check_ccmode, encrypt_with_fixed_key, isecurity_base64_encode

Function `ib_decrypt_with_fixed_key` implements the fixed key decryption using EVP_aes_128_cbc or EVP_des_ede3_cbc ciphers, calls check_ccmode, isecurity_base64_decode, decrypt_with_fixed_key

They are used in the following modules:

/products/dns/server/src/lib/msdnsonedbsync/common.c
/products/dns/server/src/lib/dns_rtxml_functions/dns_keytab.c
/products/dns/server/src/pyutil/fixd_key_encrypt.c
/products/dns/server/src/bin/make_dtc_conf/make_healthd_conf.c
/products/dns/server/src/bin/make_dhcpd_conf/mdc_common_global_handler.c
/products/dns/server/src/bin/make_bind_conf/mbc_zone_handler.c
/products/dns/server/src/bin/make_bind_conf/mbc_global_handler.c
/products/dns/server/src/bin/util/response_log_normalizer.c
/products/dns/server/src/bin
/util/ibutil/ibutil.c
/products/one/server/src/lib/one_authenticate/one_authenticate.c
/products/one/server/src/lib/onedb_util/db_dump.c
/products/one/server/src/lib/pki/ipki_store.c
/products/one/server/src/lib/pki/ipki_api.c
/products/one/server/src/lib/pki/ipki_gen.c
/products/one/server/src/lib/one_rtxml_functions/radius.c
/products/one/server/src/pyabs/auto_provision.py
/products/one/server/src/pydb/onedbmodule.c
/products/one/server/src/window/autoprov_admin_passwd_change.c
/products/one/server/src/win/auto_prov_ssl_server.c
/dhcp3/server/infoblox_gss_tsig.c
/common/server/src/lib/rtxml-query/rtxml.c
/common/server/src/lib/kerberos/keytab.c
/common/server/src/lib/onedb/trashcan.c
/common/server/src/lib/onedb/onedb_validation_cache.c
/common/server/src/lib/onedb/sqlengine.c
/common/server/src/lib/db/object.c
/common/server/src/lib/security/security_functions.c

used in function `ib_nthash_pwd`
<table>
<thead>
<tr>
<th>Directory</th>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>common</td>
<td>./common/server/src/lib/security/license.c</td>
<td>OpenSSL C-functions EVP_sha512, X509_digest, X509_free</td>
</tr>
<tr>
<td></td>
<td>./common/server/src/lib/security/supacc.c</td>
<td></td>
</tr>
<tr>
<td></td>
<td>./common/server/src/lib/mdxml/mdxml_struct_callback.c</td>
<td></td>
</tr>
<tr>
<td></td>
<td>./common/server/src/pyutil/ibutil.c</td>
<td></td>
</tr>
<tr>
<td></td>
<td>./common/server/src/pyutil/util.py</td>
<td></td>
</tr>
<tr>
<td>common</td>
<td>./common/server/src/lib/mdxml/mdxml_struct_callback.c</td>
<td>function get_new_hash - helper function which does a lazy calculation of a SHA512 fingerprint of a given certificate, it is finally used in function mdxml_convert_keys_for_certificates - final processing for certificates: one.ca_cert, one.app_certificate and one.x509_certificate will use a SHA512 fingerprint as a key instead of MD5 on issuer+serial.</td>
</tr>
<tr>
<td>ciscoise_syncd</td>
<td>./products/dns/server/src/bin/ciscoise_syncd/ciscoise_sync.c</td>
<td>OpenSSL C-functions (SSL connection) SSL_CTX_set_default_passwd_cb_userdata, SSL_CTX_use_certificate_chain_file, SSL_CTX_use_PrivateKey_file, SSL_CTX_load_verify_locations, SSL_CTX_set_verify</td>
</tr>
<tr>
<td></td>
<td>./products/dns/server/src/bin/ciscoise_syncd/ciscoise_onedb.c</td>
<td>OpenSSL C-function EVP_DecodeBlock, it decodes a block of characters of base 64 d</td>
</tr>
</tbody>
</table>
Function openssl_install_locks installs openssl thread locks
Function openssl_uninstall_locks uninstalls openssl thread locks
Function x509_cache_certificate reads the certificate from a file to X509 structure and stores the certificate in the cache
Function x509_cache_private_key reads the private key from a file to X509 structure and stores the private key in the cache
Function openssl_setup_context loads into ctx a certificate, private key, cipher list and sets message callback functions
Function openssl_set_verify_context verifies a certificate and optionally hostname
Function x509_free_cache frees certificatea and private keys cache

These functions are used in the following modules:
/products/bind/server/src/lib/healthd_private/healthd_conf.c
/products/bind/server/src/bin/idns_healthd/healthd.c
/products/bind/server/src/bin/idns_healthd/sip_monitor.c
/products/bind/server/src/bin/idns_healthd/http_monitor.c
/products/bind/server/src/bin/idns_healthd/monitor_common.c
/products/bind/server/src/lib/healthd_private/openssl_common.c

SSL context, X509 certificate functions:
SSL_CTX_use_certificate
SSL_CTX_use_certificate_file
SSL_CTX_use_PrivateKey
SSL_CTX_use_PrivateKey_file
SSL_CTX_set_cipher_list
SSL_CTX_set_msg_callback
SSL_CTX_set_msg_callback_arg
SSL_CTX_set1_param
SSL_CTX_set_verify
SSL_CTX_load_verify_locations
X509_VERIFY_PARAM_new
X509_VERIFY_PARAM_set1_host
X509_VERIFY_PARAM_free

OpenSSL C-functions: SSL_load_error_strings, SSL_library_init, OpenSSL_add_all_algorithms

SSL library init, OpenSSL_add_all_algorithms

Functions sip_task_data_init, http_task_data_init initialize OpenSSL context, calls functions
openssl_set_verify_context, openssl_setup_context

Functions sip_task_data_free, http_task_data_free frees OpenSSL context, calls function simple_connection_shutdown
They are used in module
/products/bind/server/src/bin/idns_healthd/monitor_common.c, functions
custom_task_data_init, custom_task_data_free
<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bufferevent_event_callback</td>
<td>Makes post-connection certificate verification, closes the connection in case of error.</td>
</tr>
<tr>
<td>simple_connection_init</td>
<td>Functions are used in modules.</td>
</tr>
<tr>
<td>simple_connection_start</td>
<td></td>
</tr>
<tr>
<td>simple_connection_close</td>
<td></td>
</tr>
<tr>
<td>simple_connection_check_closed</td>
<td></td>
</tr>
<tr>
<td>simple_connection_free</td>
<td></td>
</tr>
<tr>
<td>simple_connection_shutdown</td>
<td></td>
</tr>
<tr>
<td>ocsp_connect_sock</td>
<td>Connects to a socket and returns a socket BIO.</td>
</tr>
<tr>
<td>ocsp_verify_via_ocsp</td>
<td>Establishes a connection to the OCSP responder, sends the request, gets a response, verifies the response.</td>
</tr>
<tr>
<td>ib_ocsp_validate_against_responder</td>
<td>Validates a certificate against a responder, it calls ocsp_verify_via_ocsp.</td>
</tr>
<tr>
<td>ib_ocsp_add_ca_cert_to_store</td>
<td>Adds a CA certificate to a store.</td>
</tr>
<tr>
<td>ib_ocsp_init_context</td>
<td>Initializes X509 store.</td>
</tr>
<tr>
<td>ib_ocsp_release_context</td>
<td>Releases X509 store.</td>
</tr>
<tr>
<td>ib_x509_verify_certificate_against_ca_cert_store</td>
<td>Decodes X509 structure and calls verify_cert_against_ca_store.</td>
</tr>
<tr>
<td>verify_cert_against_ca_store</td>
<td>Verifies a certificate against a CA store.</td>
</tr>
<tr>
<td>ib_x509_validate_cert_against_ca_store</td>
<td>Validates a certificate against a CA store, it calls ocsp_load_ca_store.</td>
</tr>
</tbody>
</table>

OpenSSL C-functions:

- SSL_get_verify_mode
- SSL_get_verify_result
- X509_verify_cert_error_string
- BIO_socket_nbio
- BIO_sock_should_retry
- BIO_new_socket
- BIO_get_fd
- BIO_should_read
- BIO_should_write
- BIO_free_all
- OCSP_REQUEST_new
- OCSP_cert_to_id
- OCSP_request_add0_id
- OCSP_request_add1_nonce
- OCSP_sendreq_new
- OCSP_sendreq_nbio
- OCSP_response_get1_basic
- OCSP_check_nonce
- OCSP_basic_verify
- OCSP_req_find_status
- OCSP_check_valic
- OCSP_REQ_CTX_free
- OCSP_REQUEST_free
- OCSP_RESP_CTX_free
- OCSP_BASICREQ_free
- sk_X509_new_null
- sk_X509_push
- sk_X509_add
- d2i_X509_AUX
- X509_verify_cert
- X509_free
- X509_verify_cert_error_string
- X509_STORE_add_cert
- X509_STORE_new
- X509_STORE_free
- X509_STORE_set_flags
- X509_STORE_CTX_new
- X509_STORE_CTX_init
- X509_STORE_CTX_get_error
- X509_STORE_CTX_free
<table>
<thead>
<tr>
<th>one/lib</th>
<th>/products/one/server/src/lib/one_rtxml_functions/radius.c</th>
</tr>
</thead>
<tbody>
<tr>
<td>These functions use MD5 hash function:</td>
<td></td>
</tr>
<tr>
<td>radius_generate_acct_request_authenticator - generates Accounting Request Authenticator,</td>
<td></td>
</tr>
<tr>
<td>radius_verify_response_authenticator - verifies the Received response authenticator,</td>
<td></td>
</tr>
<tr>
<td>radius_encrypt_user_password - encrypts User-Password,</td>
<td></td>
</tr>
<tr>
<td>radius_encode_chap_password - encodes CHAP-Password</td>
<td></td>
</tr>
<tr>
<td>These functions use HMAC function:</td>
<td></td>
</tr>
<tr>
<td>radius_generate_message_authenticator - generates a message authenticator,</td>
<td></td>
</tr>
<tr>
<td>radius_verify_message_authenticator - verifies a message authenticator</td>
<td></td>
</tr>
<tr>
<td>they are used in module:</td>
<td></td>
</tr>
<tr>
<td>/products/one/server/src/lib/one_rtxml_functions/radius.c, functions</td>
<td></td>
</tr>
<tr>
<td>radius_verify_response_packet, radius_access_request,</td>
<td></td>
</tr>
<tr>
<td>radius_redo_access_request, radius_accounting_start,</td>
<td></td>
</tr>
<tr>
<td>admin_radius_accounting_test</td>
<td></td>
</tr>
<tr>
<td>OpenSSL hash and hmac C-functions:</td>
<td></td>
</tr>
<tr>
<td>MD5_Init, MD5_Update, MD5_Final</td>
<td></td>
</tr>
<tr>
<td>used in functions</td>
<td></td>
</tr>
<tr>
<td>radius_generate_acct_request_authenticator</td>
<td></td>
</tr>
<tr>
<td>radius_verify_response_authenticator</td>
<td></td>
</tr>
<tr>
<td>radius_encrypt_user_password</td>
<td></td>
</tr>
<tr>
<td>radius_encode_chap_password</td>
<td></td>
</tr>
<tr>
<td>EVP_md5, HMAC_Init, HMAC_Update,</td>
<td></td>
</tr>
<tr>
<td>HMAC_Final, HMAC_CTX_cleanup,</td>
<td></td>
</tr>
<tr>
<td>HMAC_cleanup</td>
<td></td>
</tr>
<tr>
<td>used in functions</td>
<td></td>
</tr>
<tr>
<td>radius_generate_message_authenticator,</td>
<td></td>
</tr>
<tr>
<td>radius_verify_message_authenticator</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>one/lib</th>
<th>/products/one/server/src/lib/one_ciscoise/one_ciscoise_functions.c</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functions _verify_cert_callback, _user_ssl_ctx_cb</td>
<td></td>
</tr>
<tr>
<td>Function _verify_cert_callback verifies a certificate using X509 functions</td>
<td></td>
</tr>
<tr>
<td>Function _user_ssl_ctx_cb verifies a certificate using SSL_CTX functions and _verify_cert_callback as callback function,</td>
<td></td>
</tr>
<tr>
<td>it is used as an argument in call of openPxGridConnection inside function</td>
<td></td>
</tr>
<tr>
<td>one_test_cisco_ise_request which tests ise connection</td>
<td></td>
</tr>
<tr>
<td>OpenSSL C-functions:</td>
<td></td>
</tr>
<tr>
<td>X509 certificate functions:</td>
<td></td>
</tr>
<tr>
<td>X509_STORE_CTX_get_error,</td>
<td></td>
</tr>
<tr>
<td>X509_STORE_CTX_get_current_cert,</td>
<td></td>
</tr>
<tr>
<td>X509_verify_cert_error_string,</td>
<td></td>
</tr>
<tr>
<td>X509_STORE_CTX_get_error_depth,</td>
<td></td>
</tr>
<tr>
<td>X509_NAME_oneline, X509_get_issuer_name, X509_get_subject_name, X509_get_serialNumber</td>
<td></td>
</tr>
<tr>
<td>used in function _verify_cert_callback</td>
<td></td>
</tr>
<tr>
<td>SSL connection functions:</td>
<td></td>
</tr>
<tr>
<td>SSL_CTX_set_default_passwd_cb_userdata,</td>
<td></td>
</tr>
<tr>
<td>SSL_CTX_use_certificate_chain_file,</td>
<td></td>
</tr>
<tr>
<td>SSL_CTX_use_PrivateKey_file,</td>
<td></td>
</tr>
<tr>
<td>SSL_CTX_load_verify_locations,</td>
<td></td>
</tr>
<tr>
<td>SSL_CTX_set_verify used in function</td>
<td></td>
</tr>
<tr>
<td>_user_ssl_ctx_cb</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>one/module</th>
<th>/products/one/server/src/module/mod_cert.c</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functions fetch_cas_by_client_cert, get_cert_san_msupn use OpenSSL functions to prepare client certificate in DER</td>
<td></td>
</tr>
<tr>
<td>Function fetch_cas_by_client_cert is used in cert_handler function</td>
<td></td>
</tr>
<tr>
<td>Function get_cert_san_msupn is used in fetch_user_by_cas_options function</td>
<td></td>
</tr>
<tr>
<td>OpenSSL C-functions:</td>
<td></td>
</tr>
<tr>
<td>BIO_new_mem_buf, BIO_free,</td>
<td></td>
</tr>
<tr>
<td>PEM_read_bio_X509, i2d_X509,</td>
<td></td>
</tr>
<tr>
<td>X509_get_issuer_name, X509_free,</td>
<td></td>
</tr>
<tr>
<td>OPENSSL_free</td>
<td></td>
</tr>
<tr>
<td>used in functions</td>
<td></td>
</tr>
<tr>
<td>fetch_cas_by_client_cert,</td>
<td></td>
</tr>
<tr>
<td>get_cert_san_msupn</td>
<td></td>
</tr>
<tr>
<td>one/bin</td>
<td>./products/one/server/src/bin/clusterd/util.c</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Functions cd_derive_serial, msg_sign256:</td>
</tr>
<tr>
<td></td>
<td>Function cd_derive_serial derives a serial number from a string (which should be the response to a handshake challenge) using SHA1 digest algorithm, it is used in modules:</td>
</tr>
<tr>
<td></td>
<td>./products/one/server/src/bin/clusterd/sendmsg_handshake.c, function cd_sendmsg_handshake_resp_req</td>
</tr>
<tr>
<td></td>
<td>./products/one/server/src/bin/clusterd/handshake.c, functions cd_master_handshake_chal, cd_potential_master_handshake_chal, cd_master_handshake_resp_chal, cd_master_handshake_resp_req, cd_potential_master_handshake_resp_req, cd_replica_handshake_resp_req, cd_replica_handshake_resp_chal</td>
</tr>
<tr>
<td></td>
<td>Function msg_sign256 signs a message with HMAC-SHA256, it is used in functions cd_sign_msg, cd_verify_msg to sign and verify a message, these functions are used in modules:</td>
</tr>
<tr>
<td></td>
<td>cd_sign_msg in ./products/one/server/src/bin/clusterd/sendmsg_handshake.c, functions cd_sendmsg_handshake_approval, cd_sendmsg_handshake_request_tunnel, cd_sendmsg_handshake_tunnel_approved, cd_sendmsg_handshake_new_master, cd_sendmsg_handshake_restart cd_verify_msg in ./products/one/server/src/bin/clusterd/handshake.c, functions cd_master_handshake_approval_verify, cd_master_handshake_tunnel_request_verify, cd_master_handshake_new_master_verify, cd_potential_master_handshake_new_master, cd_replica_handshake_approval, cd_replica_handshake_tunnel_approved, cd_replica_handshake_restart</td>
</tr>
<tr>
<td></td>
<td>OpenSSL C-functions: EVP_MD_CTX_init, EVP_sha1, EVP_DigestInit, EVP_DigestUpdate, EVP_DigestFinal, EVP_MD_CTX_cleanup used in function cd_derive_serial HMAC_CTX_init, EVP_sha256, HMAC_Init, HMAC_Update, HMAC_Final, HMAC_CTX_cleanup used in function msg_sign256</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>one/bin</th>
<th>./products/one/server/src/bin/make_syslog_conf/main.c</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Function msc_write_syslog_ng_conf writes to syslog_ng configuration file based on the information fetched from database, it is used in function main, it uses d2i_X509 to decode a certificate in DER format, X509_subject_name_hash to get hash of the X509 subject</td>
</tr>
<tr>
<td></td>
<td>OpenSSL C-functions: d2i_X509, X509_subject_name_hash, X509_free</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>one/bin</th>
<th>./products/one/server/src/bin/monitor/CHTTPMonitor.c</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Function New_CHTTPMonitor initializes a new monitor, it is used in module ./products/one/server/src/bin/monitor/main.c, function setup_monitor, it uses SSL_library_init, SSL_load_error_strings, BIO_new_fp to initialize OpenSSL</td>
</tr>
<tr>
<td></td>
<td>Function PerformHTTPsTransaction checks to see if the https is really running, it is used in function Monitor_CHTTPMonitor, it uses SSL/TLS connection functions to send HTTP request and read the server's response</td>
</tr>
<tr>
<td></td>
<td>OpenSSL C-functions: SSL_library_init, SSL_load_error_strings, BIO_new_fp used in function New_CHTTPMonitor SSLv23_method, SSL_CTX_new, SSL_new, SSL_set_fd, SSL_set_connect_state, SSL_connect, SSL_write, SSL_get_error, SSL_read, SSL_shutdown, SSL_free, SSL_CTX_free used in function PerformHTTPsTransaction</td>
</tr>
</tbody>
</table>
| one/bin | /products/one/server/src/bin/serial_console/set.c | OpenSSL C-functions: BIO_new_socket, BIO_free, BIO_new, BIO_s_mem, BIO_read, BIO_puts, BIO_new_fp, BIO_printf
| Function check_ssl_connection checks SSL connection using SSL/TLS connection functions with TLSv1 client method |
| Function download_gm_certificate downloads the GM certificate using SSL/TLS connection functions |
| Function printf_certificate prints certificate data to stdout |
| They are used in modules: |
| /products/one/server/src/bin/serial_console/set.c, function set_token |
| /products/one/server/src/bin/serial_console/show.c, function show_token (only printf_certificate) |

| one/bin | /products/one/server/src/bin/process_manager/pm_check.c | OpenSSL C-functions: MD5_Init, MD5_Update, MD5_Final |
| Function query_check checks query using MD5 hash function and callback function objhash_cb |

| one/bin | /products/one/server/src/bin/lib_prngd/main.c | OpenSSL C-functions: HMAC_CTX_init, HMAC_Init_ex, HMAC_Update, HMAC_Final, HMAC_CTX_cleanup, EVP_sha1 |
| Function hmac_sha1 does the HMAC(key, v, output) calculation with SHA-1 in one go, it is used in functions hmac_drbg_generate, hmac_drbg_update |

<p>| one/bin | /products/one/server/src/bin/show_safenet_keylabel/show_safenet_keylabel.c | OpenSSL C-functions: BIO_new_file, BIO_gets, BIO_free |
| Function luna_getprop reads property value from config file, it is used in function show_label_libname |</p>
<table>
<thead>
<tr>
<th>one/bin</th>
<th>./products/one/server/src/bin/infoblox_crypt/infoblox_crypt.c</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functions encrypt, decrypt do cryptographic encryption and decryption using EVP_bf_ofb Blowfish or EVP_aes_256_cbc AES cipher in CC mode</td>
<td></td>
</tr>
<tr>
<td>Functions sign, verify do a digital signature and verify it using MD5 or SHA256 in CC mode</td>
<td></td>
</tr>
<tr>
<td>They are used in function main</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OpenSSL C-functions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVP_CIPHER_CTX_init, EVP_DecryptInit,</td>
</tr>
<tr>
<td>EVP_DecryptUpdate, EVP_DecryptFinal,</td>
</tr>
<tr>
<td>EVP_aes_256_cbc, EVP_bf_ofb,</td>
</tr>
<tr>
<td>EVP_CIPHER_CTX_cleanup used in function encrypt</td>
</tr>
<tr>
<td>EVP_CIPHER_CTX_init, EVP_EncryptInit,</td>
</tr>
<tr>
<td>EVP_EncryptUpdate, EVP_EncryptFinal,</td>
</tr>
<tr>
<td>EVP_aes_256_cbc, EVP_bf_ofb,</td>
</tr>
<tr>
<td>EVP_CIPHER_CTX_cleanup used in function decrypt</td>
</tr>
<tr>
<td>EVP_VerifyInit, EVP_VerifyUpdate,</td>
</tr>
<tr>
<td>EVP_VerifyFinal, EVP_sha256,</td>
</tr>
<tr>
<td>EVP_md5, EVP_PKEY_free, PEM_read_X509_get_pubkey used in function verify</td>
</tr>
<tr>
<td>EVP_MD_CTX_init, EVP_SignInit,</td>
</tr>
<tr>
<td>EVP_SignUpdate,</td>
</tr>
<tr>
<td>EVP_SignFinal, EVP_sha256, EVP_md5,</td>
</tr>
<tr>
<td>EVP_MD_CTX_cleanup, EVP_PKEY_free, PEM_read_PrivateKey used in function sign</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>one/bin</th>
<th>./products/one/server/src/bin/util/auto_prov_ssl_client.c</th>
</tr>
</thead>
<tbody>
<tr>
<td>./products/one/server/src/bin/util/auto_prov_ssl_server.c</td>
<td></td>
</tr>
<tr>
<td>Function select_read reads bytes from a TLS/SSL connection, it is used in functions handshake, main, Servlet</td>
<td></td>
</tr>
<tr>
<td>Function handshake does server/client protocol negotiation, it calls function select_read and writes bytes to a TLS/SSL connection, it is used in function main, Servlet</td>
<td></td>
</tr>
<tr>
<td>Function LoadCertificates loads the first certificate stored in file into ctx, then checks the consistency of a private key with the corresponding certificate loaded into ctx, it is used in InitCTX, InitServerCTX</td>
<td></td>
</tr>
<tr>
<td>Functions InitCTX, InitServerCTX initialize SSL context</td>
<td></td>
</tr>
<tr>
<td>Function Servlet makes SSL connection with client, it is used in function main</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OpenSSL C-functions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL_get_fd, SSL_read used in function select_read</td>
</tr>
<tr>
<td>SSL_write used in function handshake</td>
</tr>
<tr>
<td>SSL_accept, SSL_write, SSL_get_fd,</td>
</tr>
<tr>
<td>SSL_free used in function Servlet</td>
</tr>
<tr>
<td>SSL_CTX_use_certificate_file,</td>
</tr>
<tr>
<td>SSL_CTX_use_PrivateKey_file,</td>
</tr>
<tr>
<td>SSL_CTX_check_private_key used in function LoadCertificates</td>
</tr>
<tr>
<td>OpenSSL_add_all_algorithms,</td>
</tr>
<tr>
<td>SSL_load_error_strings, TLSv1_client_method,</td>
</tr>
<tr>
<td>TLSv1_server_method, SSL_CTX_new,</td>
</tr>
<tr>
<td>SSL_CTX_set_verify, SSL_CTX_set_cipher,</td>
</tr>
<tr>
<td>SSL_CTX_load_verify_locations used in functions InitCTX, InitServerCTX</td>
</tr>
<tr>
<td>SSL_library_init, SSL_new, SSL_set_fd,</td>
</tr>
<tr>
<td>SSL_connect, SSL_write, SSL_free,</td>
</tr>
<tr>
<td>SSL_CTX_free used in function main</td>
</tr>
<tr>
<td>Directory</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>one/bin</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>one/bin</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>one/bin</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>atp</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>ifmap</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Function tcp_connect sets SSL session, connection, checks server credentials when required
Function tcp_disconnect shuts down a SSL connection, releases SSL context
Function soap_poll polls SSL connection socket, it uses SSL_peek which does not remove bytes from the underlying BIO during the read
They are used in modules:
./products/ifmap/server/src/lib/gsoap/stdsoap2.c
./products/ifmap/server/src/lib/gsoap/dom.c
./products/ifmap/server/src/lib/ifmap/client/ifmap20_operations.c
./products/ifmap/server/src/lib/ifmap/client/ifmap_operations.c
./products/ifmap/server/src/lib/ifmap/metadata.c

X509_verify_cert_error_string,
SSL_get_peer_certificate,
X509_free used in function soap_ssl_accept
SSL_SESSION_free, SSL_free,
SSL_CTX_free used in function soap_done
SSL_new, SSL_clear, SSL_connect,
SSL_set_session, SSL_SESSION_free,
BIO_new_socket, SSL_set_bio,
SSL_get_error, SSL_get_verify_result,
X509_verify_cert_error_string,
SSL_get_peer_certificate,
X509_get_ext_count, X509_get_ext,
X509_EXTENSION_get_object,
X509v3_EXT_get, X509v3_conf_free,
X509_get_subject_name,
X509_NAME_get_index_by_NID,
X509_NAME_get_entry,
OPENSSL_free, X509_free
used in function tcp_connect
SSL_SESSION_free, SSL_get1_session,
SSL_shutdown, SSL_get_error,
SSL_free used in function tcp_disconnect
SSL_peek used in function soap_poll
SSL_CTX_new, SSLv23_method,
SSL_CTX_load_verify_locations,
SSL_CTX_set_client_CA_list,
SSL_load_client_CA_file,
SSL_CTX_set_default_verify_paths,
SSL_CTX_use_certificate_chain_file,
SSL_CTX_set_default_passwd_cb_userdata
SSL_CTX_set_default_passwd_cb,
SSL_CTX_use_PrivateKey_file,
SSL_CTX_set_options, SSL_CTX_set_verify
SSL_CTX_set_verify_depth
RSA_generate_key(1024, RSA_F4,...),
SSL_CTX_set_tmp_rsa, RSA_free, BIO_new
BIO_free, PEM_read_bio_DHparams,
SSL_CTX_set_temp_dh, DH_free
used in function ssl_auth_init
X509_STORE_CTX_get_error,
<table>
<thead>
<tr>
<th>Module</th>
<th>Function/Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifmap</td>
<td>./products/ifmap/server/src/lib/gsoap/th-lock.c</td>
</tr>
<tr>
<td></td>
<td>Functions CRYPTO_thread_setup, CRYPTO_thread_cleanup setups and cleanups openssl thread locks</td>
</tr>
<tr>
<td></td>
<td>They are used in module</td>
</tr>
<tr>
<td></td>
<td>./products/ifmap/server/src/lib/ifmap/client/ifmap_operations.c, functions</td>
</tr>
<tr>
<td></td>
<td>ifmap_init_client_lib, ifmap_release_client_lib</td>
</tr>
<tr>
<td></td>
<td>OpenSSL thread support C-functions:</td>
</tr>
<tr>
<td></td>
<td>CRYPTO_num_locks,</td>
</tr>
<tr>
<td></td>
<td>CRYPTO_set_id_callback,</td>
</tr>
<tr>
<td></td>
<td>CRYPTO_set_locking_callback,</td>
</tr>
<tr>
<td></td>
<td>CRYPTO_set_dynlock_create_callback,</td>
</tr>
<tr>
<td></td>
<td>CRYPTO_set_dynlock_lock_callback,</td>
</tr>
<tr>
<td></td>
<td>CRYPTO_set_dynlock_destroy_callback</td>
</tr>
<tr>
<td>ifmap</td>
<td>./products/ifmap/server/src/lib/ifmap/client/ifmap_operations.c</td>
</tr>
<tr>
<td></td>
<td>Function ifmap_init_client - set cipher list for ccmode, it is used in function</td>
</tr>
<tr>
<td></td>
<td>ifmap_client_connect, modules:</td>
</tr>
<tr>
<td></td>
<td>./products/ifmap/server/src/bin/ifmapcd/client.c</td>
</tr>
<tr>
<td></td>
<td>./ifmap/server/src/bin/ifmapcd/client.c</td>
</tr>
<tr>
<td></td>
<td>OpenSSL C-functions:                                                         SSL_CTX_set_cipher</td>
</tr>
<tr>
<td>Python code</td>
<td>./products/netmri/server/src/pyutil/cert_util.py</td>
</tr>
<tr>
<td></td>
<td>Function check_discovery_node checks and regenerate if needed node certificate and node private key file, it is used in modules:</td>
</tr>
<tr>
<td></td>
<td>./products/netmri/server/src/bin/util/anp_vpn_client.py, function start</td>
</tr>
<tr>
<td></td>
<td>./products/netmri/server/src/bin/util/anm_vpn_server.py, function start</td>
</tr>
<tr>
<td></td>
<td>Package M2Crypto functions:</td>
</tr>
<tr>
<td></td>
<td>X509.load_cert</td>
</tr>
<tr>
<td>Python code</td>
<td>./products/netmri/server/src/pyutil/make_discovery_configuration.py</td>
</tr>
<tr>
<td></td>
<td>Function cisco_apic_configurations_add_element uses hashlib.md5 to convert 'uuid' (128 bits) to integer of 31 bits, it is used in function unit_settings_add_element</td>
</tr>
<tr>
<td></td>
<td>Package hashlib functions:</td>
</tr>
<tr>
<td></td>
<td>hashlib.md5</td>
</tr>
<tr>
<td>Python code</td>
<td>./products/gog/server/src/pyabs/sso.py</td>
</tr>
<tr>
<td></td>
<td>Function sign signs token data, it is used in function get_sso_info</td>
</tr>
<tr>
<td></td>
<td>Function _verify verifies SSO Token, it is used in UTs</td>
</tr>
<tr>
<td></td>
<td>Package M2Crypto functions:</td>
</tr>
<tr>
<td></td>
<td>SMIME.load_key, sign, verify, set_x509_stack, set_x509_store, load_pkcs7_bio</td>
</tr>
<tr>
<td></td>
<td>X509.X509_Socket, X509_Store BIO.MemoryBuffer</td>
</tr>
</tbody>
</table>
### Python code

**./products/gog/server/src/pyutil/cert_util.py**

Function `create_temp_cert` creates a temporary certificate (generates an RSA key pair with key length of 2048 bits, public and sign key with md=SHA1), it is used in function `make_join_file`

Function `make_join_file` returns join token, it is used in module **./products/gog/server/src/pyutil/gog_common.py**, function `get_join_info`

Function `m2_generate_and_encode_csr` generates signed request, private and public key, it is used in functions `gen_ca_cert`, `check_mgm_cert`, `check_node`, `check_sso`

Function `m2_sign_csr` returns signed certificate, it is used in function `gen_ca_cert`

Function `m2_sign_csr_by_ca` returns signed by CA certificate, it is used in functions `check_mgm_cert`, `check_node`, `check_sso`, `sign_csr`

Function `m2_create_req` creates a X509 certificate request, it is used in functions `create_temp_cert`, `m2_generate_and_encode_csr`

Function `m2_create_cert_and_sign` creates a certificate from a request and sign it, it is used in functions `create_temp_cert`, `m2_sign_csr`, `m2_sign_csr_by_ca`

Function `m2_b64_str_to_rsa` feeds a pem string to RSA, it is used in functions `m2_generate_and_encode_csr`, `m2_sign_csr`, `m2_sign_csr_by_ca`

**/products/gog/server/src/pyutil/sgm_daemon_util.py**

Function `DBTask.execute_connect` handles connect request from subgrid, it is used in `DBTask.__init__` to initialize an action map

Function `GoGListenerMsg.__create_digest` signs a digest with the private key using SHA256, it is used in `GoGListenerMsg.send_msg`

**/products/gog/server/src/pyutil/external_storage_connection.py**

Function `SignatureWrapper.reset` initializes a signature by a new hmac object with digestmod = SHA256, `SignatureWrapper` is the base class of classes `HTTPResponseWrapper`, `BufferWrapper`, `FileWrapper`, `FileWrapper`, `BufferWrapper`

### Package M2Crypto functions:

- RSA.gen_key, RSA.load_key
- EVP.PKey with md=SHA1 by default
- X509.load_cert, load_request_string, load_cert_string, Request
- X509_Name, set_serial_number, set_version, set_subject, set_issuer, set_pubkey, set_not_before, set_not_after, sign
- ASN1.ASN1_UTCTIME

### Package M2Crypto functions:

- X509.load_cert_string

### Package hashlib functions:

- hashlib.sha256

### Package hmac functions:

- hmac.new
<table>
<thead>
<tr>
<th>Python code</th>
<th>.products/gog/server/src/pyutil/join_file.py</th>
<th>Package hmac functions: hmac.new</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function create_password creates a password using the supplied cert and join token, it is used in modules: .products/gog/server/src/pyutil/cert_util.py, function make_join_file .products/one/server/src/pyutil/subgrid.py, function _check_join_info</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Python code</th>
<th>.products/reporting/server/src/bin/util/splunk_backup.py</th>
<th>Package hashlib functions: hashlib.sha256</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function append_checksum appends checksum SHA256 to the content, it is used in function backup</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Python code</th>
<th>.products/reporting/server/src/pyabs/reporting_util.py</th>
<th>Openssl command: openssl ca -notext -batch -config os.path.join (dirname,'ca.conf') -in os.path.join(dirname,'csr.pem') -out os.path.join(dirname,'cert.pem')</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function sign_certificate_request signs incoming certificate signing request using CA certificate, it is used in module .products/one/server/src/wapi/reporting.py, function sign_certificate_func_call</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Python code</th>
<th>.products/dns/server/src/pyutil/util.py</th>
<th>Package hashlib functions: hashlib.new('md5')</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function get_zone_file_name generates zone file name from zonekey using MD5, it is used in modules: .products/dns/server/src/pyabs/named_db_files.py, function NamedDBFilesReaderOneDB._add_files .products/dns/server/src/bin/util/rpz_last_update_time.py, function zone_update</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Function add_idns_certificate adds the idns certificate, it is used in modules: .products/dns/server/src/wapi/dtc.py, class WAPISObject_dtc_2_6, WFFuncCall('add_certificate',...) .products/dns/server/src/ibap/idnsfuncs.py, AddIdnsCertificate.execute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function _unpack_openssl_cipher_list converts an OpenSSL cipher list string to the equivalent list of individual cipher suite strings, it is used in functions _get_slow_cipher_list, validate_cipher_list</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Python code</th>
<th>.products/one/server/src/cloudinit-gpl/sources/DataSourceIBAzure.py</th>
<th>Openssl commands: openssl x509 -noout -pubkey (along with ssh-keygen -i -m PKCS8 -f /dev/stdin)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function crtfile_to_pubkey extracts a public key from a certificate into format PKCS8, it is used in function pubkeys_from_crt_files</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Python code</td>
<td>Package hashlib functions:</td>
<td>Package hmac functions:</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>./products/one/server/src/aws_gateway/aws_out_req.py</td>
<td>hashlib.sha256</td>
<td>hmac.new (digestmod=SHA256)</td>
</tr>
<tr>
<td>Function _get_signed_header returns a header containing a signature, used</td>
<td></td>
<td></td>
</tr>
<tr>
<td>in function OutRequest.perform</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./products/one/server/src/aws_gateway/aws_auth.py</td>
<td>hashlib.sha256</td>
<td>hmac.new (digestmod=SHA256)</td>
</tr>
<tr>
<td>Function sign signs a message, used in function getSignatureKey</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function AwsSignatureBase.createStringToSign,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>it is used in functions AwsSignatureV4InHdr.parseAmzHdrs,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AwsSignatureV4InData.parseAmzHdrs,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function AwsSignatureBase.verify verifies a signature, used in function</td>
<td></td>
<td></td>
</tr>
<tr>
<td>authenticate_aws_req</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function AwsSignatureV2InData.verify verifies a signature, used in function</td>
<td></td>
<td></td>
</tr>
<tr>
<td>authenticate_aws_req</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./products/one/server/src/admin_conn/wapibase.py</td>
<td>hmac.HMAC</td>
<td>(digestmod=SHA1)</td>
</tr>
<tr>
<td>Function PagingPageID._hmac signs data with HMAC-SHA1, used in class</td>
<td></td>
<td></td>
</tr>
<tr>
<td>functions dump, load</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./products/one/server/src/admin_conn/userauth.py</td>
<td>M2Crypto set_x509_stack, load_pkcs7_bio</td>
<td>hmac.HMAC</td>
</tr>
<tr>
<td>Function AuthInfo.__sso_verify verifies SSO token, used in class function</td>
<td></td>
<td>(digestmod=SHA256, MD5)</td>
</tr>
<tr>
<td>__check_sso_token</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function AuthInfo.generate_proxy_auth generates the proxy authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>header, used in class function is_proxy_auth_code_valid</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function AuthChallenge.verify verifies auth challenge, used in AuthInfo.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>checkmac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./products/one/server/src/admin_conn/cryptfuncs.py</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function _compute_ssha computes the special IB SHA1 passwd hash, used in</td>
<td>hmac.HMAC</td>
<td>(digestmod=SHA1, MD5)</td>
</tr>
<tr>
<td>function ispasswordsequal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./products/one/server/src/pyabs/syslog_config.py</td>
<td>openssl x509 -noout -hash -in filename</td>
<td></td>
</tr>
<tr>
<td>Function get_certificate_hash_from_file gets a certificate hash from a file,</td>
<td>openssl x509 -in cert_file -noout -ocsp_uri</td>
<td></td>
</tr>
<tr>
<td>it is used in functions make_symlink_to_certificate,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>create_full_certificate_file_path</td>
<td></td>
<td></td>
</tr>
<tr>
<td>./products/one/server/src/pyabs/ocsp_auth.py</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function OcspAuthService.__get_responders_from_aia gets OCSP responder</td>
<td>openssl x509 -in cert_file -noout -ocsp_uri</td>
<td></td>
</tr>
<tr>
<td>address(es) from aia, used in class function __get_effective_responders</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Python code</td>
<td>./products/one/server/src/pyabs/certificate.py</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Function import_http_cert imports http certificate, used in function upload_certificate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function key_len_verify verifies key length is greater than 2048, it is used in functions one_generate_and_export_csr, one_assign_self_signed_certificate, import_http_cert, import_eap_ca_cert, import_ifmap_ca_cert, import_tae_ca_cert, import_server_cert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function _substract_public_key extracts a public key from a certificate, used in function _handle_gen_tlsa_certificate_data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Openssl commands: x509, pkey
openssl x509 -purpose -noout -in data_ref.get('data')
openssl x509 -inform DER -pubkey -noout -ir
openssl pkey -pubin -outform DER -in outfile
Package M2Crypto functions:
X509.load_cert_string,
x509.get_pubkey
Package hashlib functions: hashlib.sha256, hashlib.sha512

<table>
<thead>
<tr>
<th>Python code</th>
<th>./products/one/server/src/pyabs/captive_portal_common.py</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function CaptivePortalHttpConfGen._is_captive_portal_ca_updated checks if the captive portal CA was updated using MD5, used in class function make_conf</td>
<td></td>
</tr>
</tbody>
</table>

Package hashlib functions: hashlib.md5

<table>
<thead>
<tr>
<th>Python code</th>
<th>./products/one/server/src/pyabs/endpoint_restapi_util.py</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function gen_endpoint_dxl_certificates generates a self-signed CA and use that to sign a client certificate, returns ca_crt, client_pem: self-signed CA and client certificates, it is used in function gen_endpoint_dxl_certificates_with_export_data_ref which is used in modules:</td>
<td></td>
</tr>
<tr>
<td>./products/one/server/src/wapi/fileops.py, function _generatedxlendpointcerts_func</td>
<td></td>
</tr>
<tr>
<td>./products/one/server/src/ibap/endpointfuncs.py, class function GenEndpointDxlCertificates.execute</td>
<td></td>
</tr>
</tbody>
</table>

Openssl commands: req, ca
openssl req -new -sha256 -nodes
-keystay ca_key -subj ca_subj -out ca_csr
openssl req -new -sha256 -nodes
-keystay client_key -subj client_subj -out client_csr
openssl ca -config ssl_cfg_file_name
-selfsign -keyfile ca_key -in ca_csr -out ca_crt
-batch -startdate startdate -enddate enddate
openssl ca -config ssl_cfg_file_name cert ca_crt
-keyfile ca_key -in client_csr -out client_crt -t
-batch -startdate startdate -enddate enddate

<table>
<thead>
<tr>
<th>Python code</th>
<th>./products/one/server/src/pyabs/hsm_safenet_group.py</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function HSMSafeNetGroup.validate_sign_algo checks the signature algo from the server certificate, used in class function restore_server_cert</td>
<td></td>
</tr>
</tbody>
</table>

Openssl command: openssl x509 -in cert_path -text

<table>
<thead>
<tr>
<th>Python code</th>
<th>./products/one/server/src/pyutil/util.py</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function generate_member_virtual_ip_md5 generates MD5 string based on member virtual ip list, Function generate_anycast_member_virtual_ip_md5 generates MD5 string based on member virtual ip list only for anycast enabled They are used in module ./products/one/server/src/pyabs/members.py, Member.check_member_changes</td>
<td></td>
</tr>
<tr>
<td>Function set_unit_serial_number set the serial number of an appliance, it uses MD5 to check secret, it is used in module ./products/one/server/src/ibap/miscfuncs.py, SetUnitSerialNumber.execute</td>
<td></td>
</tr>
<tr>
<td>Function get_spki_hash returns sha256 hash of Subject Public Key Info of the given cert, used in function revoked</td>
<td></td>
</tr>
<tr>
<td>Function get_subject_dn returns issuer DN of the given cert, used in function revoked</td>
<td></td>
</tr>
<tr>
<td>Function get_ssl_tls_cipher_suites_mapping returns dict with key - cipher_suite name used by DB and value as cipher suite name used by openssl, used in get_default_cipher_suites_httpd_directive</td>
<td></td>
</tr>
</tbody>
</table>

Package hashlib functions: hashlib.md5

Openssl commands: x509, rsa, sha256
openssl x509 -text -sha256
openssl x509 -pubkey -noout
openssl x509 -subject -noout
openssl rsa -pubin -outform DER
openssl sha256
<table>
<thead>
<tr>
<th>Python code</th>
<th>Package M2Crypto functions</th>
<th>Package ssl functions</th>
<th>Package M2Crypto functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>./products/one/server/src/pyutil/subgrid.py</td>
<td>Function _check_join_info verifies join_file and join_token, it verifies the private key matches the public key in the certificate and the certificate is signed by the CA (with SHA1) it is used in function join_gog and module ./products/one/server/src/ibap/subgridfuncs.py, FetchGridNameBeforeJoin.execute</td>
<td>X509.load_cert_string, get_pubkey RSA.load_key_string, sign, verify PKey.get_rsa</td>
<td></td>
</tr>
<tr>
<td>./products/one/server/src/pyutil/checked_https_handler.py</td>
<td>Function CheckedHTTPSConnection.connect checks server cert against CA List and cert expiry date, server cert purpose, server cert matches hostname being accessed, the class is used in CheckedHTTPSHandler.https_open</td>
<td>Package ssl functions: wrap_socket</td>
<td>X509.load_cert_string, SSL.Checker</td>
</tr>
<tr>
<td>./products/one/server/src/pyutil/tae_util.py</td>
<td>Function register registers this system with an associated TAE system for automation, it requires a certificate from the server, it is used in module ./products/one/server/src/ibap/miscfuncs.py, TaeRegister.execute</td>
<td>Package ssl functions: wrap_socket</td>
<td></td>
</tr>
<tr>
<td>./products/one/server/src/bin/util/gog_listener.py</td>
<td>Function AttachHandler.verify_digest verifies MGM certificate with SHA256, used in class function handle</td>
<td>Package hashlib functions:</td>
<td>hashlib.sha256().update Package M2Crypto functions: X509.get_pubkey, PKey.get_rsa, RSA.verify</td>
</tr>
<tr>
<td>./products/one/server/src/bin/util/member_registration_client.py</td>
<td>Function HTTPServerAuthConnection.connect connects to a host on a given SSL port, the class is used in NodeRegistration.call Function validate_ssl_certificate validates the certificate contained in the given pem file, used in function main</td>
<td>Package ssl functions: wrap_socket</td>
<td>Package M2Crypto functions: X509.load_cert</td>
</tr>
<tr>
<td>./products/one/server/src/bin/util/startup_integrity_test.py</td>
<td>Function generate_key_and_certificate generates a private key and certificate, used in function main Function _gen_sha256sums generates a checksum for each executable file, used in function generate_sha256sums which used in main Function check_sha256sums extracts the public key from the certificate, verifies checksum file signature and checksums, used in function main</td>
<td>openssl commands: req, dgst, x509 openssl req -nodes -x509 -sha256 -newkey rsa:4096 -keyout self.private_key_path -out self.certificate_path -batch openssl dgst -sha256 -sign self.private_key -out self.dgst_file self.checksum_file openssl x509 -in self.certificate_path -pubkey openssl dgst -sha256 -verify pubkey_path -signature self.dgst_file self.checksum_file (along with sha256sum --quiet -c self.checksum_file)</td>
<td></td>
</tr>
<tr>
<td>./products/one/server/src/bin/util/check_vpn_cert_expiry.py</td>
<td>Function node_cert_expired returns 'true' if the vpn cert will expire in 120 days from now else 'false', used in function main</td>
<td>Package M2Crypto functions: X509.load_cert</td>
<td></td>
</tr>
<tr>
<td>./products/one/server/src/outbound/lib/ssl_wrapper.py</td>
<td>Class WrapSSLSocket is derived from ssl.SSLSocket which provides a socket-like wrapper that also encrypts and decrypts the data going over the socket with SSL, it is used in WrapHTTPSConnection.connect to connect to a host on a given SSL port</td>
<td>Package ssl class: ssl.SSLSocket</td>
<td></td>
</tr>
<tr>
<td>Python code</td>
<td>Path to file</td>
<td>Function description</td>
<td>Package functions</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------</td>
<td>----------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>/products/ifmap/server/src/bin/util/check_ifmap_client_conf.py</td>
<td>Function make_ifmap_client_config creates a file holding DHCP IF-MAP client configuration, calculates a password hash by MD5, used in function main</td>
<td>Package hashlib functions: hashlib.md5</td>
<td></td>
</tr>
<tr>
<td>/vnios/dnsfw_util/product_activation.py</td>
<td>Function main among other things generates HASH using HMAC_SHA256 algorithm and API_KEY as salt/privateKey</td>
<td>Package hashlib functions: hashlib.sha256, hmac.new (digestmod=SHA256)</td>
<td></td>
</tr>
<tr>
<td>/common/server/src/pyutil/util.py</td>
<td>Function file_md5_checksum calculates md5 checksum for a file, it is used in module /products/gog/server/src/pyabs/nios_image.py, NiosImage.insert</td>
<td>Package hashlib functions: hashlib.md5</td>
<td></td>
</tr>
<tr>
<td>/common/server/src/pyutil/libsguenforce.py</td>
<td>Function GenericParser.init_md5 initializes md5 class member, used in derived class MessageParser, function typedef_struct_state</td>
<td>Package hashlib functions: hashlib.md5</td>
<td></td>
</tr>
<tr>
<td>/common/server/src/libbyamz/auth.py</td>
<td>Function payload_digest creates a hash of a payload (http-request body) with SHA256, used in function canonical_request</td>
<td>Package hashlib functions: hashlib.sha256, hmac.new (digestmod=SHA256)</td>
<td></td>
</tr>
<tr>
<td>Bash script</td>
<td>Path to file</td>
<td>Function canonical_requestigest creates a hash of a canonical request string with SHA256, used in function string_to_sign</td>
<td></td>
</tr>
<tr>
<td>/products/reporting/server/src/bin/util/make_splunk_certs.sh</td>
<td>These functions are used to create splunk certificates and pem files</td>
<td>'openssl' command</td>
<td></td>
</tr>
<tr>
<td>Bash script</td>
<td>Function to restore</td>
<td>'openssl' command</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------</td>
<td>-------------------</td>
<td></td>
</tr>
<tr>
<td>.products/reporting/server/src/bin/util/splunk_app_common.sh</td>
<td>splunk_app_data_restore()</td>
<td>openssl dgst -sha256 -hmac $REPORTING_HMAC_KEY $spl_filename openssl dgst -sha256 -hmac $REPORTING_HMAC_KEY $(TAR_FILE) &gt; $(TAR_FILE).sha256&quot;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bash script</th>
<th>For certificat expiry check</th>
<th>'openssl' command</th>
</tr>
</thead>
<tbody>
<tr>
<td>.products/one/server/src/bin/util/check_cert_expire.sh</td>
<td>openssl x509 -in $ARGV -noout -text</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bash script</th>
<th>To check the vpn certificate date</th>
<th>'openssl' command</th>
</tr>
</thead>
<tbody>
<tr>
<td>.products/one/server/src/bin/util/check_vpn_cert_dates.sh</td>
<td>openssl x509 -noout -in $NODE_CRT_FILE</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bash script</th>
<th>1. To get GM end date 2. To get the appliance end date 3. To get GM CaCert.pem end date 4. To get the appliance CaCert.pem end date</th>
<th>'openssl' command</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Bash script</th>
<th>This function is called through /infoblox/one/bin/check_cert_expire</th>
<th>'openssl' command</th>
</tr>
</thead>
<tbody>
<tr>
<td>.products/one/server/src/bin/util/validate_server_cert.sh</td>
<td>openssl x509 -in $ARGV -noout -text</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bash script</th>
<th>To retrieve remote certificate</th>
<th>'openssl' command</th>
</tr>
</thead>
<tbody>
<tr>
<td>.products/one/server/src/bin/util/retrieve_remote_certificate.sh</td>
<td>openssl verify $(CERT_FILE) &gt;/dev/null 2&gt;&amp;1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bash script</th>
<th>Generate a DNS RR from an x.509 certificate</th>
<th>'openssl' command</th>
</tr>
</thead>
<tbody>
<tr>
<td>.bind9/contrib/dane/mkdane.sh</td>
<td>openssl x509 -in &quot;$IN&quot; -inform &quot;$FORM&quot; -out openssl dgst -sha256 openssl dgst -sha512</td>
<td></td>
</tr>
</tbody>
</table>
Bash script

```
Function GenNodeCert()
1. Generating key for node
2. Generating CSR for node
3. Signing certificate for node
4. Generating DH key
```

```
1. `openssl` command
   1. `openssl genrsa -out $KDIR/node${CERTNAME}.key 2048`
   2. `openssl req -new -key $KDIR/node${CERTNAME}.key -out $CDIR/node${CERTNAME}.req -outform PEM -config $CDIR/vpngen${CERTNAME}.conf -batch`
   3. `openssl ca -keyfile $PKEY -batch -notext -in $CDIR/node${CERTNAME}.req -cert $PCERT -config $CDIR/vrca.conf -key infoblox -out $KDIR/node${CERTNAME}.crt -startdate 040101000000Z -enddate 371231235959Z`
   4. `openssl dhparam -out $KDIR/dh.pem 2048`
```

Bash script

```
Function generate-mf()
    Dumps the SHA1 fingerprints of ovf and vmdk files to the .mf file
    `openssl` command
    `openssl sha1`
```

Bash script

```
The below files dont have openssl command in it
. /strip_aslan_root.sh
. /remove_packages.sh
. /products/one/server/src/bin/util/one_common.sh
```

HSM

```
Primarily used for DNSSEC
modules which use OpenSSL functions:
. /products/one/server/src/pyabs/hsm_safenet_group.py
Function HSMSafeNetGroup.validate_sign_algo checks the signature algo from the server certificate, it is used in HSMSafeNetGroup.restore_server_cert which is used in insert, update
```

Openssl command: `openssl x509 -in cert_path -text`

**Appendix E Regular Expressions**

**Supported Expressions for Search Parameters**

Regular expressions are text strings that you use to describe search patterns. You can use the following special characters to define regular expressions for search parameters.

<table>
<thead>
<tr>
<th>Special character</th>
<th>Purpose</th>
<th>Example</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>()</td>
<td>Defines the scope and precedence of the operator</td>
<td>gr(a(e)y)</td>
<td>Matches “gray” or “grey”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Matches either the regular expression before or after the vertical bar</td>
<td>a</td>
<td>c</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Matches any single character</td>
<td>.at</td>
<td>Matches any text string ending with “at”, such as “hat”, “cat”, and “bat”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>Matches the previous regular expression zero or more times</td>
<td>a*bc</td>
<td>Matches zero or multiple occurrences of “a” followed by “bc”, such as “bc”, “abc”, “aabbc”, “aabc”, and so on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+</td>
<td>Matches the previous regular expression one or more times</td>
<td>a+bc</td>
<td>Matches one or more occurrences of “a”, followed by “bc”,”abc”, “aabbc”, “aabc”, and so on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>?</td>
<td>Matches the previous regular expression zero or one time</td>
<td>a?bc</td>
<td>Matches zero or one occurrence of “a”, followed by “bc”, such as “bc” or “abc”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>^</td>
<td>Matches the beginning of a text string</td>
<td>^c</td>
<td>Matches any string beginning with “c”, such as “cat”.</td>
</tr>
</tbody>
</table>
$  Matches the end of a text string
com$  Matches any string ending with "com", such as "Infoblox.com".

[ ]  Matches any character specified in the brackets
[03] [abcd] [1a-d]  Matches 0" or 3.

[ n-n]  Matches single characters contained in the specified range, including the start and end points
[0-3] [a-f]  Matches 0, 1, 2, and 3.

\(m,n\)  Matches the preceding expression at least m but not more than n times.
a\(\{3,5\}\)  Matches "aaa", "aaaa", and "aaaaa".

Note: You can change a special character—such as the period (.), asterisk (*), plus sign (+), or question mark (?)—into a literal character by prefixing it with a backslash (\). For example, to specify a literal period, asterisk, plus sign, or question mark, use the characters within the following parentheses: (\.), (\*), (\+), (?), (\^), (\$).

Appendix F NIOS Virtual Appliances

NIOS virtual appliances support most of the features of the Infoblox NIOS software, with some limitations. This appendix describes these limitations. Table E.1 summarizes the supported NIOS virtual appliance models.

Note: VMware Tools are automatically installed for each NIOS virtual appliance. Infoblox supports the control functions in Hyper-V Manager and VMware Tools. For example, through the vSphere client, you can shut down the virtual appliance.

Table E.1 Supported NIOS virtual Appliance Models and Specifications

<table>
<thead>
<tr>
<th>NIOS Virtual Appliances</th>
<th>Primary Disk (GB)</th>
<th># of CPU Cores</th>
<th>Memory Allocation (GB)</th>
<th>Virtual CPU Core Frequency Limit</th>
<th>NIOS for VMware</th>
<th>NIOS for MS Hyper-V</th>
<th>NIOS for Xen</th>
<th>NIOS for KVM</th>
<th>NIOS for AWS</th>
<th>Supported as Grid Master and Grid</th>
</tr>
</thead>
<tbody>
<tr>
<td>IB-VM-100</td>
<td>55</td>
<td>1</td>
<td>1</td>
<td>1300 MHz</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>No</td>
</tr>
<tr>
<td>IB-VM-800 (for reporting only; 1 GB daily limit)</td>
<td>300 (Primary &amp; Reporting)</td>
<td>2</td>
<td>Range: 4 – 8 Default: 8</td>
<td>3000 MHz</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>Yes</td>
</tr>
<tr>
<td>IB-VM-800 (for reporting only; 2 GB daily limit)</td>
<td>300 (Primary &amp; Reporting)</td>
<td>2</td>
<td>Range: 4 – 8 Default: 8</td>
<td>3000 MHz</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>No</td>
</tr>
<tr>
<td>IB-V805 * (Reporting only)</td>
<td>250 (+ 1 TB user defined reporting storage)</td>
<td>2</td>
<td>32</td>
<td>N/A</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>No</td>
</tr>
<tr>
<td>IB-VM-810</td>
<td>55</td>
<td>2</td>
<td>2</td>
<td>2000 MHz</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>No</td>
</tr>
<tr>
<td>IB-VM-810</td>
<td>160</td>
<td>2</td>
<td>2</td>
<td>2000 MHz</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>No</td>
</tr>
<tr>
<td>IB-V815 *</td>
<td>250</td>
<td>2</td>
<td>16</td>
<td>N/A</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>Yes</td>
</tr>
<tr>
<td>IB-VM-820</td>
<td>55</td>
<td>2</td>
<td>4</td>
<td>3000 MHz</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>Yes</td>
</tr>
<tr>
<td>IB-VM-820</td>
<td>160</td>
<td>2</td>
<td>4</td>
<td>3000 MHz</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>Yes</td>
</tr>
<tr>
<td>IB-V825 *</td>
<td>250</td>
<td>2</td>
<td>16</td>
<td>N/A</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>Yes</td>
</tr>
<tr>
<td>IB-VM-1400 (for reporting only; 5 GB daily limit)</td>
<td>555 (Primary &amp; Reporting)</td>
<td>4</td>
<td>Default: 8 GB</td>
<td>8000 MHz</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>No</td>
</tr>
<tr>
<td>IB-V1405 * (Reporting only)</td>
<td>250 (+ 1.2 TB user defined reporting storage)</td>
<td>4</td>
<td>32</td>
<td>N/A</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>No</td>
</tr>
<tr>
<td>IB-VM-1410</td>
<td>55</td>
<td>4</td>
<td>8 GB</td>
<td>6000 MHz</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>IB-VM-1410 *</td>
<td>160</td>
<td>4</td>
<td>8</td>
<td>6000 MHz</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Yes²</td>
</tr>
<tr>
<td>IB-V1415 *</td>
<td>250</td>
<td>4</td>
<td>32</td>
<td>N / A</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Yes</td>
</tr>
<tr>
<td>IB-VM-1420</td>
<td>160</td>
<td>4</td>
<td>8</td>
<td>8000 MHz</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Yes²</td>
</tr>
<tr>
<td>IB-V1425 *</td>
<td>250</td>
<td>4</td>
<td>32</td>
<td>N / A</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Yes</td>
</tr>
<tr>
<td>IB-V2205 * (Reporting only)</td>
<td>250 (+ 2.4 TB user defined reporting storage)</td>
<td>8</td>
<td>64</td>
<td>N / A</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>IB-VM-2210</td>
<td>160</td>
<td>4</td>
<td>12</td>
<td>12000 MHz</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Yes²</td>
</tr>
<tr>
<td>IB-V2215 *</td>
<td>250</td>
<td>8</td>
<td>64</td>
<td>N / A</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Yes</td>
</tr>
<tr>
<td>IB-VM-2220</td>
<td>160</td>
<td>4</td>
<td>12</td>
<td>12000 MHz</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Yes²</td>
</tr>
<tr>
<td>IB-V2225 *</td>
<td>250</td>
<td>8</td>
<td>64</td>
<td>N / A</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Yes</td>
</tr>
<tr>
<td>IB-V4000 (Reporting only)</td>
<td>250 (+ 1500 GB reporting storage)</td>
<td>8</td>
<td>24</td>
<td>2400 MHz</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>IB-V4005 (Reporting only)</td>
<td>250 (+ user defined reporting)</td>
<td>14</td>
<td>128</td>
<td>2400 MHz</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>IB-V4015</td>
<td>250</td>
<td>14</td>
<td>128</td>
<td>2400 MHz</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Yes</td>
</tr>
<tr>
<td>IB-V4025</td>
<td>250</td>
<td>14</td>
<td>128</td>
<td>2400 MHz</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Yes</td>
</tr>
<tr>
<td>IB-V5005** User defined reporting storage</td>
<td>User defined</td>
<td>User defined</td>
<td>N / A</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Insight Virtual Appliances</th>
<th>Overall Disk (GB)</th>
<th># of CPU Cores</th>
<th>Memory Allocation (GB)</th>
<th>Virtual CPU Core Frequency Limit</th>
<th>NIOS for VMware</th>
<th>NIOS for AWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ND-V800</td>
<td>160</td>
<td>2</td>
<td>8</td>
<td>3000 MHz</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ND-V805 *5</td>
<td>250</td>
<td>2</td>
<td>32</td>
<td>N / A</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ND-V1400</td>
<td>160</td>
<td>4</td>
<td>16</td>
<td>8000 MHz</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ND-V1405 *5</td>
<td>250</td>
<td>4</td>
<td>32</td>
<td>N / A</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ND-V2200</td>
<td>160</td>
<td>8</td>
<td>24</td>
<td>24000 MHz</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ND-V2205 *5</td>
<td>250</td>
<td>8</td>
<td>32</td>
<td>N / A</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ND-V4005</td>
<td>250</td>
<td>14</td>
<td>128</td>
<td>2400 MHz</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cloud Platform Virtual Appliances</th>
<th>Overall Disk (GB)</th>
<th># of CPU Cores</th>
<th>Memory Allocation (GB)</th>
<th>Virtual CPU Core Frequency Limit</th>
<th>NIOS for VMware</th>
<th>NIOS for MS Hyper-V</th>
<th>Nios for Xen</th>
<th>NIOS for KVM</th>
<th>NIOS for AWS</th>
<th>Supported as Grid Master and Grid Master Candidate</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-V800</td>
<td>160</td>
<td>2</td>
<td>2</td>
<td>2000 MHz</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>CP-V1400</td>
<td>160</td>
<td>4</td>
<td>8</td>
<td>6000 MHz</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
<tr>
<td>CP-V2200</td>
<td>160</td>
<td>4</td>
<td>12</td>
<td>12000 MHz</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>No</td>
</tr>
</tbody>
</table>

**NOTES:**

- You can freely assign resources to these virtual appliances to suit your business needs, as long as the resources are within the limits of the licenses being installed on the appliances.

1For KVM hypervisor only. Not supported for KVM-based OpenStack. Does not support Elastic Scaling.

2NIOS virtual appliance for Hyper-V is not recommended as a Grid Master or Grid Master Candidate. IB-VM-820 with 55 GB disk is not supported as the Grid Master or Grid Master Candidate for the NIOS virtual for KVM. The Identity Mapping feature is supported on the IB-VM-810 and IB-VM-820 appliances only if they are configured as Grid members, not as the Grid Master.
Does not support Elastic Scaling.

NIOS for KVM is supported in the following environments: OpenStack, RHEL, SuSE Enterprise and Cloud, and CentOS. Note that only IB-V1405 as a Reporting server has been qualified for OpenStack.

ND virtual appliances are designed for Network Insight only. Discovery is supported in OpenStack only with SRIOV enabled. For information about the limitations on each NIOS virtual appliance, see the following:

- NIOS for Riverbed
- NIOS for VMware
- NIOS for Hyper-V
- NIOS for Xen

NIOS for Riverbed

NIOS virtual appliances on Riverbed have the following limitations:

- They can function as Grid members only. You cannot configure them as HA (high availability) pairs, Grid Masters, Grid Master candidates, or independent appliances.
- On a Grid with a NIOS virtual appliance on Riverbed as a Grid member, the maximum storage space for HTTP, FTP and TFTP is 1 GB (a Grid with only Infoblox appliances provides a maximum of 5 GB for these services), core files are 100 MB each, and syslog and infoblox.log files are 20 MB each. Scheduled backup file is 100 MB.
- The LAN interface is the only network interface available on the NIOS virtual appliance. You cannot configure the speed and transmission type (full or half duplex) of the network interface.
- You can use the traffic capture tool of the NIOS virtual software package to capture traffic only on the LAN port of the NIOS virtual appliance.
- NIOS virtual appliances on Riverbed do not support the following features:
  - Anycast addressing
  - Configuration as a DHCP lease history logging member
  - Dedicated MGMT port
  - NTP service
  - bloxTools environment
  - Configuration for managing Microsoft® Windows DNS servers

NIOS for VMware

The Infoblox NIOS for VMware can also run on Cisco SRE-V (Services Ready Engine Virtualization), which is part of the Cisco UCS (Unified Computing System) Express. For more information about NIOS virtual for VMware, refer to the Infoblox Installation Guide for NIOS Software on VMware.

NIOS virtual for VMware appliances support most of the features of the Infoblox NIOS appliances, with the following limitations:

- You must have a NIOS virtual license installed on the appliance before you can access the Infoblox GUI.
- NIOS virtual appliances do not support the following features:
  - Configuration of port settings for MGMT, LAN, LAN2, and HA ports
  - The bloxTools environment
  - The IB-BOB virtual appliance is supported on Cisco SRE-V and can function as a Grid member only. It does not support configuration as an independent appliance, an HA pair, a Grid Master, or a Grid Master candidate. It also does not support access to the Infoblox GUI.
  - The IB-VM-250 virtual appliance supports all the services provided by NIOS virtual appliances, but it is not recommended as a Grid Master or Grid Master candidate.
  - When you configure an HA pair, both nodes in the HA pair must be NIOS instances. You cannot configure a physical NIOS appliance and a NIOS virtual instance in an HA pair.
  - NIOS virtual appliances run on virtual hardware. They do not have sensors to monitor the physical CPU temperature, fan speed, and system temperature.
  - Changing the NIOS virtual appliance settings through the VMware vSphere or vCenter console may violate the terms of the NIOS virtual licensing and support models. The NIOS virtual appliance may not join the Grid or function properly.

NIOS for Hyper-V

NIOS virtual for Microsoft Windows 2008 R2 and 2012 R2 server appliances support most of the features of the Infoblox NIOS appliances, with the following limitations:

- You must have a NIOS virtual license installed on the appliance before you can access the Infoblox GUI.
- NIOS virtual appliances do not support the following features:
  - Configuration of port settings for MGMT, LAN, LAN2, and HA ports
  - The bloxTools environment
  - All the IB-VM appliance models support all the services provided by NIOS virtual appliances, but Grid Master or Grid Master Candidate is not supported.
  - The Captive Portal is supported only on IB-VM-1410 virtual appliances.
  - NIOS virtual appliances run on virtual hardware. They do not have sensors to monitor the physical CPU temperature, fan speed, and system temperature.
  - Changing the NIOS virtual appliance settings through the Hyper-V Manager or Virtual Machine Manager Administrator console may violate the terms of the NIOS virtual licensing and support models. The NIOS virtual appliance may not join the Grid or function properly.
NIOS for Xen

NIOS virtual appliance for Xen supports most of the features of the Infoblox NIOS appliances, with the following limitations:

- NIOS virtual appliances do not support the following features:
  - Configuration of port settings for MGMT, LAN, LAN2, and HA ports
  - The bloxTools environment
- When you configure an HA pair, both nodes in the HA pair must be NIOS virtual instances. You cannot configure a physical NIOS appliance and a NIOS virtual instance in an HA pair.
- NIOS virtual appliances run on virtual hardware. They do not have sensors to monitor the physical CPU temperature, fan speed, and system temperature.
- Changing the NIOS virtual appliance settings through the NIOS virtual for Xen virtual appliance console may violate the terms of the NIOS virtual licensing and support models. The NIOS virtual appliance may not join the Grid or function properly.

Appendix G Product Compliance

This appendix describes the hardware components, requirements, and specifications, plus agency and RFC (Request for Comments) compliance for the Infoblox appliance. Topics in this appendix include:

- Power Safety Information
- AC
- DC
- Agency Compliance
  - FCC
  - Canadian Compliance
- RFC Compliance
  - DNS RFC Compliance
  - DHCP RFC Compliance
  - DHCPv6 RFC Compliance
  - IDN (Internationalized Domain Names) RFC Compliance

Power Safety Information

The main external power connector for the Infoblox appliance is located on the back of the system. Ensure power to the system is off before connecting the power cord into the power connector. Please read the following power safety statements for your AC- or DC-powered appliance:

AC

English

**WARNING:** This product relies on the building’s installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120VAC, 15A U.S. (240VAC, 10A international) is used on the phase conductors (all current-carrying conductors).

French

**WARNING:** Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l’installation électrique du local. Vérifier qu’un fusible ou qu’un disjoncteur de 120V alt., 15A U.S. maximum (240V alt., 10A international) est utilisé sur les conducteurs de phase (conducteurs de charge).

German

**WARNING:** Dieses Produkt ist darauf angewiesen, daß im Gebäude ein Kurzschluß - bzw. Überstromschutz installiert ist. Stellen Sie sicher, daß eine Sicherung oder ein Unterbrecher von nicht mehr als 240V Wechselstrom, 10A (bzw. in den USA120V Wechselstrom, 15A) an den Phasenleitern (allen Stromf, hrenden Leitern) verwendet wird.

DC

English

**WARNING:** When stranded wiring is required, use approved wiring terminations, such as closed-loop or spade-type with upturned lugs. These ter
Agency Compliance

The Infoblox appliance is compliant with these EMI and safety agency regulations:

<table>
<thead>
<tr>
<th>Standard</th>
<th>Agency</th>
<th>Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCC Part 15</td>
<td>FCC</td>
<td>FCC</td>
</tr>
<tr>
<td>EN55022, EN55024, EN61000-3-2, EN61000-3-3</td>
<td>TUV</td>
<td>CE</td>
</tr>
<tr>
<td>UL60950/CSA60950</td>
<td>UL</td>
<td>cULus</td>
</tr>
<tr>
<td>EN60950</td>
<td>TUV</td>
<td>GS</td>
</tr>
<tr>
<td>CB Scheme</td>
<td>IECEE</td>
<td>Report and Certificate IEC 60950-1:2001</td>
</tr>
<tr>
<td>VCCI-A</td>
<td>VCCI</td>
<td>VCCI</td>
</tr>
<tr>
<td>AS/NZS 3548</td>
<td>ACMA</td>
<td>C-Tick</td>
</tr>
</tbody>
</table>

**FCC**

The FCC label on the back of the system indicates this network appliance is compliant with limits for a Class A digital device in accordance with Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when this equipment is operated in a commercial environment. Operation is subject to the following two conditions:

- This device might not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This device generates, uses, and can radiate radio frequency energy if not installed and used in accordance with the instructions in this manual. Operating this equipment in a residential area is likely to cause harmful interference, and the customer will be required to rectify the interference at his or her own expense. This product requires the use of external shielded cables to maintain compliance pursuant to Part 15 of the FCC Rules.

**Canadian Compliance**

**English**

This Class A digital apparatus complies with Canadian ICES-003.

**French**

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

**VCCI**

The Infoblox appliance complies with this VCCI regulation (compliance statement follow by its translation):

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the Technical Requirements of the Voluntary Control Council for Interference Technology (VCCI). In a domestic environment this product may cause radio interference, in which case the user may be required to take corrective action.

**Caution**: Lithium battery included with this board. Do not puncture, mutilate, or dispose of battery in fire. Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by manufacturer. Dispose of used battery according to manufacturer instructions and in accordance with your local regulations.
RFC Compliance

The NIOS appliance is compliant with the following:

- Qualys and Nessus security requirements
- Joint Interoperability Test Command (JITC) certification for Internet Protocol version 6 capability
- RFCs (Request for Comments):
  - DNS RFC Compliance
  - DHCP RFC Compliance
  - DHCPv6 RFC Compliance
  - IDN (Internationalized Domain Names) RFC Compliance

DNS RFC Compliance

The NIOS appliance complies with the following DNS RFCs:

Table F.2 RFCs for DNS

<table>
<thead>
<tr>
<th>RFC Number</th>
<th>RFC Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>805</td>
<td>Computer Mail Meeting Notes</td>
</tr>
<tr>
<td>811</td>
<td>Hostnames Server</td>
</tr>
<tr>
<td>819</td>
<td>The Domain Naming Convention for Internet User Applications</td>
</tr>
<tr>
<td>881</td>
<td>The Domain Names Plan and Schedule</td>
</tr>
<tr>
<td>882</td>
<td>Domain Names: Concepts and Facilities</td>
</tr>
<tr>
<td>883</td>
<td>Domain Names: Implementation Specification</td>
</tr>
<tr>
<td>897</td>
<td>Domain Name System Implementation Schedule</td>
</tr>
<tr>
<td>920</td>
<td>Domain Requirements</td>
</tr>
<tr>
<td>921</td>
<td>Domain Name System Implementation Schedule – Revised</td>
</tr>
<tr>
<td>973</td>
<td>Domain System Changes and Observations</td>
</tr>
<tr>
<td>974</td>
<td>Mail Routing and the Domain System</td>
</tr>
<tr>
<td>1032</td>
<td>Domain Administrators Guide</td>
</tr>
<tr>
<td>1033</td>
<td>Domain Administrators Operations Guide</td>
</tr>
<tr>
<td>1034</td>
<td>Domain Names – Concepts and Facilities</td>
</tr>
<tr>
<td>1035</td>
<td>Domain Names – Implementation and Specification</td>
</tr>
<tr>
<td>1101</td>
<td>DNS Encoding of Network Names and Other Types</td>
</tr>
<tr>
<td>1122</td>
<td>Requirements for Internet Hosts – Communication Layers</td>
</tr>
<tr>
<td>1123</td>
<td>Requirements for Internet Hosts – Application and Support</td>
</tr>
<tr>
<td>1178</td>
<td>Choosing a Name for Your Computer</td>
</tr>
<tr>
<td>1348</td>
<td>DNS NSAP RRs</td>
</tr>
<tr>
<td>1386</td>
<td>The US Domain</td>
</tr>
<tr>
<td>1464</td>
<td>Using the Domain Name System to Store Arbitrary String Attributes</td>
</tr>
<tr>
<td>1535</td>
<td>A Security Problem and Proposed Correction with Widely Deployed DNS Software</td>
</tr>
<tr>
<td>1536</td>
<td>Common DNS Implementation Errors and Suggested Fixes</td>
</tr>
<tr>
<td>1537</td>
<td>Common DNS Data File Configuration Errors</td>
</tr>
<tr>
<td>1591</td>
<td>Domain Name System Structure and Delegation</td>
</tr>
<tr>
<td>Page</td>
<td>Title</td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>1611</td>
<td>DNS Server MIB Extensions</td>
</tr>
<tr>
<td>1612</td>
<td>DNS Resolver MIB Extensions</td>
</tr>
<tr>
<td>1637</td>
<td>DNS NSAP Resource Records</td>
</tr>
<tr>
<td>1664</td>
<td>Using the Internet DNS to Distribute RFC</td>
</tr>
<tr>
<td>1327</td>
<td>Mail Address Mapping Tables</td>
</tr>
<tr>
<td>1713</td>
<td>Tools for DNS debugging</td>
</tr>
<tr>
<td>1794</td>
<td>DNS Support for Load Balancing</td>
</tr>
<tr>
<td>1811</td>
<td>U.S. Government Internet Domain Names</td>
</tr>
<tr>
<td>1816</td>
<td>U.S. Government Internet Domain Names</td>
</tr>
<tr>
<td>1912</td>
<td>Common DNS Operational and Configuration Errors</td>
</tr>
<tr>
<td>1956</td>
<td>Registration in the MIL Domain</td>
</tr>
<tr>
<td>1982</td>
<td>Serial Number Arithmetic</td>
</tr>
<tr>
<td>1995</td>
<td>Incremental Zone Transfer in DNS</td>
</tr>
<tr>
<td>1996</td>
<td>A Mechanism for Prompt Notification of Zone Changes</td>
</tr>
<tr>
<td>2010</td>
<td>Operational Criteria for Root Name Servers</td>
</tr>
<tr>
<td>2052</td>
<td>A DNS RR for specifying the location of services (DNS SRV)</td>
</tr>
<tr>
<td>2053</td>
<td>The AM (Armenia) Domain</td>
</tr>
<tr>
<td>2136</td>
<td>Dynamic Updates in the Domain Name System (DNS UPDATE)</td>
</tr>
<tr>
<td>2142</td>
<td>Mailbox Names for Common Services, Roles and Functions</td>
</tr>
<tr>
<td>2146</td>
<td>U.S. Government Internet Domain Names</td>
</tr>
<tr>
<td>2168</td>
<td>Resolution of Uniform Resource Identifiers using the Domain Name System</td>
</tr>
<tr>
<td>2181</td>
<td>Clarifications to the DNS Specification</td>
</tr>
<tr>
<td>2182</td>
<td>Selection and Operation of Secondary DNS Servers</td>
</tr>
<tr>
<td>2219</td>
<td>Use of DNS Aliases for Network Services</td>
</tr>
<tr>
<td>2240</td>
<td>A Legal Basis for Domain Name Allocation</td>
</tr>
<tr>
<td>2308</td>
<td>Negative Caching of DNS Queries (DNS NCACHE)</td>
</tr>
<tr>
<td>2317</td>
<td>Classless IN-ADDR.ARPA Delegation</td>
</tr>
<tr>
<td>2352</td>
<td>A Convention for Using Legal Names as Domain Names</td>
</tr>
<tr>
<td>2537</td>
<td>RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)</td>
</tr>
<tr>
<td>2606</td>
<td>Reserved Top Level DNS Names</td>
</tr>
<tr>
<td>2782</td>
<td>A DNS RR for Specifying the Location of Services (DNS SRV)</td>
</tr>
<tr>
<td>2845</td>
<td>Secret Key Transaction Authentication for DNS (TSIG)</td>
</tr>
<tr>
<td>2915</td>
<td>The Naming Authority Pointer (NAPTR) DNS Resource Record</td>
</tr>
<tr>
<td>2930</td>
<td>Secret Key Establishment for DNS (TKEY RR)</td>
</tr>
<tr>
<td>3596</td>
<td>DNS Extensions to Support IP Version 6</td>
</tr>
<tr>
<td>3645</td>
<td>Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)</td>
</tr>
<tr>
<td>3768</td>
<td>Virtual Router Redundancy Protocol (VRRP)</td>
</tr>
</tbody>
</table>
DHCP RFC Compliance

The appliance complies with the following DHCP RFCs:
Table F.3 RFCs for DHCP

<table>
<thead>
<tr>
<th>RFC Number</th>
<th>RFC Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1531</td>
<td>Dynamic Host Configuration Protocol 1534 Interoperation Between DHCP and BOOTP</td>
</tr>
<tr>
<td>1542</td>
<td>Clarifications and Extensions for the Bootstrap Protocol</td>
</tr>
<tr>
<td>2131</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>2132</td>
<td>DHCP Options and BOOTP Vendor Extensions</td>
</tr>
<tr>
<td>3046</td>
<td>DHCP Relay Agent Information Option</td>
</tr>
<tr>
<td>3315</td>
<td>Dynamic Host Configuration Protocol for IPv6 (DHCPv6)</td>
</tr>
<tr>
<td>3925</td>
<td>Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)</td>
</tr>
<tr>
<td>4388</td>
<td>Dynamic Host Configuration Protocol (DHCP) Leasequery</td>
</tr>
</tbody>
</table>

DHCPv6 RFC Compliance

The appliance complies with the following DHCPv6 RFCs:
Table F.4 RFCs for DHCPv6

<table>
<thead>
<tr>
<th>RFC Number</th>
<th>RFC Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>4075</td>
<td>Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6</td>
</tr>
<tr>
<td>3898</td>
<td>Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)</td>
</tr>
<tr>
<td>3736</td>
<td>Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6</td>
</tr>
<tr>
<td>3646</td>
<td>DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)</td>
</tr>
<tr>
<td>3633</td>
<td>IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6</td>
</tr>
</tbody>
</table>
IDN (Internationalized Domain Names) RFC Compliance

The appliance complies with the following IDN RFCs:
Table F.5 RFCs for IDN

<table>
<thead>
<tr>
<th>RFC Number</th>
<th>RFC Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>3492</td>
<td>Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)</td>
</tr>
<tr>
<td>5890</td>
<td>International Domain Names for Applications (IDNA): Definitions and Document Framework</td>
</tr>
<tr>
<td>5891</td>
<td>International Domain Names for Applications (IDNA): Background, Explanation, and Rationale</td>
</tr>
<tr>
<td>5892</td>
<td>The Unicode code points and IDNA</td>
</tr>
<tr>
<td>5893</td>
<td>Right-to-left scripts for IDNA</td>
</tr>
<tr>
<td>5894</td>
<td>International Domain Names in Applications (IDNA): Protocol</td>
</tr>
<tr>
<td>5895</td>
<td>Mapping Characters in IDNA2008</td>
</tr>
<tr>
<td>6452</td>
<td>The Unicode Code Points and Internationalized Domain Names for Applications (IDNA) - Unicode 6.0</td>
</tr>
</tbody>
</table>

Appendix H Open Source Copyright and License Statements

Infoblox has made every attempt to adhere to the guidelines for use and contribution to the open source community. Please report back to Infoblox any suspected violations of the copyrights, use of open source contributions via the distribution of binaries and/or source from Infoblox. It is the intent of Infoblox to comply with the open source rules of use, and comply with the various copyrights found in the distribution of the products from Infoblox.

This appendix contains the copyright notices for the binary-only distribution from Infoblox. Source changes are contributed back to the open source community when the copyright holder states this is desired. As stated by the enclosed copyrights, a copy of open source files used in our binary-only distribution is available from Infoblox. There is a nominal cost to obtain a CD containing the source files, to cover our costs of duplication and distribution. To obtain a copy of the source, contact us via e-mail at info@infoblox.com, or call us at 1.408.625.4200. The sections in this appendix include:

- GNU General Public License
- GNU Lesser General Public License
- Apache Software License, Version 2.0
- ISC BIND Copyright
- ISC DHCP Copyright
- Julian Seward Copyright
- Carnegie Mellon University Copyright
- Thai Open Source Software Center Copyright
- Ian F. Darwin Copyright
- Lawrence Berkeley Copyright
- MIT Kerberos Copyright
- BSD License
- David L. Mills Copyright
- OpenLDAP License
- OpenSSL License
- VIM License
- ZLIB License
- Wietse Venema Copyright
- ECLIPSE SOFTWARE
- Eclipse Public License - v 1.0
- AOP Alliance (Java/J2EE AOP standards)
- OpenJDK
- TASM
- Distributed Computing Laboratory, Emory University
- COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL)
- The FreeType Project LICENSE
- The Independent JPEG Group's JPEG software
- Net-SNMP
- The PHP License, version 3.01
- INFO-ZIP
- MIT License
- Ehcache
GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundations software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each authors protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyones free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Programs source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be 11 distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License is to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and any later version, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to
ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

GNU Lesser General Public License

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages-typically libraries-of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original authors reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.
We call this license the “Lesser” General Public License because it does Less to protect the users freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification").

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Librarys complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions

   a. The modified work must itself be a software library.
   b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
   c. You must cause the whole of the work to be licensed at nocharge to all third parties under the terms of this License.
   d. If a facility in the modified Library refers to a function or a table of data to be supplied by an appropriate program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can
4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source code along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customers own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of the following things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can manage the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the users computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities.

b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, redistribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues),
DISTRIBUTION

Apache Software License, Version 2.0

Copyright (c) 2004 The Apache Software Foundation. All rights reserved. TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensors" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity.

For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

END OF TERMS AND CONDITIONS

Apache Software License, Version 2.0

Copyright (c) 2004 The Apache Software Foundation. All rights reserved. TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensors" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).
“Derivative Works” shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated into the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   a. You must give any other recipients of the Work or Derivative Works a copy of this License; and
   b. You must cause any modified files to carry prominent notices stating that You changed the files; and
   c. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
   d. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

perl Artistic License

The "Artistic License"

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

"Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

"Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder as specified below.

"Copyright Holder" is whoever is named in the copyright or copyrights for the package.

"You" is you, if you're thinking about copying or distributing this Package.

"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:
   a. place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.
   b. use the modified Package only within your corporation or organization.
   c. rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.
   d. make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:
   a. distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.
   b. accompany the distribution with the machine-readable source of the Package with your modifications.
c. give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.
d. make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own. You may embed this Packages interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called "undump" or "unexec" methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package nor shall it fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this Package.

7. C subroutines (or comparably compiled subroutines in other languages) supplied by you and linked into this Package in order to emulate subroutines and variables of the language defined by this Package shall not be considered part of this Package, but are the equivalent of input as in Paragraph 6, provided these subroutines do not change the language in any way that would cause it to fail the regression tests for the language.

8. Aggregation of this Package with a commercial distribution is always permitted provided that the use of this Package is embedded; that is, when no overt attempt is made to make this Packages interfaces visible to the end user of the commercial distribution. Such use shall not be construed as a distribution of this Package.

9. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

10. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

ISC BIND Copyright

Copyright (C) 1996-2002 Internet Software Consortium.
Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.
THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright (C) 1996-2001 Nomimum, Inc.
Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.
THE SOFTWARE IS PROVIDED "AS IS" AND NOMINUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

ISC DHCP Copyright

Copyright (c) 1995, 1996, 1997, 1998, 1999 Internet Software Consortium -DHCP. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of Internet Software Consortium - DHCP nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY INTERNET SOFTWARE CONSORTIUM AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward Copyright

This program, "bzip2" and associated library "libbzip2", are copyright (C) 1996-2002 Julian R Seward. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, Cambridge, UK.
jseward@acm.org
bzip2/libbzip2 version 1.0.2 of 30 December 2001

Carnegie Mellon University Copyright
Copyright (c) 2001 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact

   Office of Technology Transfer
   Carnegie Mellon University
   5000 Forbes Avenue
   Pittsburgh, PA 15213-3890
   (412) 268-4387, fax: (412) 268-7395
   tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)."

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Thai Open Source Software Center Copyright
Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper

Copyright (c) 2001, 2002 Expat maintainers.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Ian F. Darwin Copyright
Software written by Ian F. Darwin and others; maintained 1994-1999 Christos Zoulas.
This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at the beginning of the file, without modification, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   This product includes software developed by Ian F. Darwin and others.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Lawrence Berkeley Copyright

Copyright (c) 1990 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Vern Paxson.

The United States Government has rights in this work pursuant to contract no.
DE-AC03-76SF00098 between the United States Department of Energy and the University of California.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

MIT Kerberos Copyright

Copyright Notice and Legal Administrivia

Copyright (C) 1985-2002 by the Massachusetts Institute of Technology. All rights reserved.

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original MIT software.

M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Individual source code files are copyright MIT, Cygnus Support, OpenVision, Oracle, Sun Soft, FundsXpress, and others.

Project Athena, Athena MUSE, Discuss, Hesiod, Kerberos, Moira, and Zephyr are trademarks of the Massachusetts Institute of Technology (MIT). No commercial use of these trademarks may be made without prior written permission of MIT.

"Commercial use" means use of a name in a product or other for-profit manner. It does NOT prevent a commercial firm from referring to the MIT trademarks in order to convey information (although in doing so, recognition of their trademark status should be given).

The following copyright and permission notice applies to the OpenVision Kerberos Administration system located in kadmin/create, kadmin/dbutil, kadmin/passwd, kadmin/server, lib/kadm5, and portions of lib/rpc:

Copyright, OpenVision Technologies, Inc., 1996. All Rights Reserved
WARNING: Retrieving the OpenVision Kerberos Administration system source code, as described below, indicates your acceptance of the following terms. If you do not agree to the following terms, do not retrieve the OpenVision Kerberos administration system.

You may freely use and distribute the Source Code and Object Code compiled from it, with or without modification, but this Source Code is provided to you "AS IS" EXCLUSIVE OF ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY OTHER WARRANTY, WHETHER EXPRESS OR IMPLIED. IN NO EVENT WILL OPENVISION HAVE ANY LIABILITY FOR ANY LOST PROFITS, LOSS OF DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM THE USE OF THE SOURCE CODE, OR THE FAILURE OF THE SOURCE CODE TO PERFORM, OR FOR ANY OTHER REASON.

OpenVision retains all copyrights in the donated Source Code. OpenVision also retains copyright to derivative works of the Source Code, whether created by OpenVision or by a third party. The OpenVision copyright notice must be preserved if derivative works are made based on the donated Source Code.

OpenVision Technologies, Inc. has donated this Kerberos Administration system to MIT for inclusion in the standard Kerberos 5 distribution. This donation underscores our commitment to continuing Kerberos technology development and our gratitude for the valuable work which has been performed by MIT and the Kerberos community.

Portions contributed by Matt Crawford <crawdad@fnal.gov> were work performed at Fermi National Accelerator Laboratory, which is operated by Universities Research Association, Inc., under contract DE-AC02-76CH03000 with the U.S. Department of Energy.
BSD License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

David L. Mills Copyright

Copyright (c) David L. Mills 1992-2003 *

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

OpenLDAP License

The OpenLDAP Public License Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices.
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

OpenSSL License

Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. ([http://www.openssl.org/](http://www.openssl.org/))"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit ([http://www.openssl.org/](http://www.openssl.org/))"
There are no restrictions on distributing an unmodified copy of Vim. Parts of Vim may also be distributed, but this text must always be included. You are allowed to include executables that you made from the unmodified Vim sources, your own usage examples and Vim scripts. If you distribute a modified version of Vim, you are encouraged to send the maintainer a copy, including the source code. Or make it available to the maintainer through ftp; let him know where it can be found. If the number of changes is small (e.g., a modified Makelife) e-mailing the diffs will do. When the maintainer asks for it (in any way) you must make your changes, including source code, available to him. The maintainer reserves the right to include any changes in the official version of Vim. This is negotiable. You are not allowed to distribute a modified version of Vim when you are not willing to make the source code available to the maintainer. The current maintainer is Bram Moolenaar <Bram@vim.org>. If this changes, it will be announced in appropriate places (most likely www.vim.org and comp.editors). When it is completely impossible to contact the maintainer, the obligation to send him modified source code ceases. It is not allowed to remove these restrictions from the distribution of the Vim sources or parts of it. These restrictions may also be used for previous Vim releases instead of the text that was included with it. Vim is Charityware. You can use and copy it as much as you like, but you are encouraged to make a donation for needy children in Uganda. Please see |kcc| below or visit the ICCF web site, available at these mirrors: http://www.vim.org/iccf/ http://www.iccf.nl/ The Open Publication License applies to the Vim documentation, see | manual - copyright |.

--- begin of license ---

VIM LICENSE

There are no restrictions on distributing unmodified copies of Vim except that they must include this license text. You can also distribute unmodified parts of Vim, likewise unrestricted except that they must include this license text. You are also allowed to include executables that you made from the unmodified Vim sources, your own usage examples and Vim scripts. It is allowed to distribute a modified (or extended) version of Vim, including executables and/or source code, when the following four conditions are met:

1. This license text must be included unmodified.
2. The modified Vim must be distributed in one of the following five ways:
   a. If you make changes to Vim yourself, you must clearly describe in the distribution how to contact you. When the maintainer asks you (in any way) for a copy of the modified Vim you distributed, you must make your changes, including source code, available to the maintainer without fee. The maintainer reserves the right to include your changes in the official version of Vim. What the maintainer will do with your changes and under what license they will be distributed is negotiable. If there has been no negotiation then this license, or a later version, also applies to your changes. The current maintainer is Bram Moolenaar <Bram @vim.org>. If this changes it will be announced in appropriate places (most likely vim.sf.net, www.vim.org and/or comp.editors). When it is completely impossible to contact the maintainer, the obligation to send him your changes ceases. Once the maintainer has confirmed that he has received your changes they will not have to be sent again.
   b. If you have received a modified Vim that was distributed as mentioned under a) you are allowed to further distribute it unmodified, as mentioned at I). If you make additional changes the text under a) applies to those changes.
   c. Provide all the changes, including source code, with every copy of the modified Vim you distribute. This may be done in the form of a context diff. You can choose what license to use for new code you add. The changes and their license must not restrict others from making their own changes to the official version of Vim.
   d. When you have a modified Vim which includes changes as mentioned under c), you can distribute it without the source code for the changes if the following three conditions are met:
      - The license that applies to the changes permits you to distribute the changes to the Vim maintainer without fee or restriction, and permits the Vim maintainer to include the changes in the official version of Vim without fee or restriction.
      - You keep the changes for at least three years after last distributing the corresponding modified Vim. When the maintainer or someone who you distributed the modified Vim to asks you (in any way) for the changes within this period, you must make them available to him.
      - You clearly describe in the distribution how to contact you. This contact information must remain valid for at least three years after last distributing the corresponding modified Vim, or as long as possible.
   e. When the GNU General Public License (GPL) applies to the changes, you can distribute the modified Vim under the GNU GPL version 2 or any later version.
3. A message must be added, at least in the output of the :version command and in the intro screen, such that the user of the modified Vim is able to see that it was modified. When distributing as mentioned under 2)e) adding the message is only required for as far as this does not conflict with the license used for the changes.
4. The contact information as required under 2)a) and 2)d) must not be removed or changed, except that the person himself can make corrections.
If you distribute a modified version of Vim, you are encouraged to use the Vim license for your changes and make them available to the maintainer, including the source code.

The preferred way to do this is by e-mail or by uploading the files to a server and e-mailing the URL. If the number of changes is small (e.g., a modified Makefile) e-mailing a context diff will do. The e-mail address to be used is <maintainer@vim.org>

It is not allowed to remove this license from the distribution of the Vim sources, parts of it or from a modified version. You may use this license for previous Vim releases instead of the license that they came with, at your option.

--- end of license ---

**ZLIB License**

(C) 1995-2002 Jean-loup Gailly and Mark Adler

This software is provided as-is, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler
jloup@gzip.org madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate not receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.

**Wietse Venema Copyright**

/* ************************************************************************ * Copyright 1995 by Wietse Venema. All rights reserved. Some individual * files may be covered by other copyrights. * * This material was originally written and compiled by Wietse Venema at * Eindhoven University of Technology, The Netherlands, in 1990, 1991, * 1992, 1993, 1994 and 1995. * * Redistribution and use in source and binary forms are permitted * provided that this entire copyright notice is duplicated in all such * copies. * * This software is provided "as is" and without any expressed or * implied * warranties, including, without limitation, the implied warranties of * merchantability and fitness for any particular purpose. * ************************************************************************/

**ECLIPSE SOFTWARE**

The product includes Eclipse software (the "Eclipse Program") provided by the Eclipse Foundation and licensed to Infoblox Inc. under the Eclipse Public License v1.0.

EXCEPT AS EXPRESSLY SET FORTH IN THE ECLIPSE PUBLIC LICENSE, THE ECLIPSE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. EXCEPT AS EXPRESSLY SET FORTH IN THE ECLIPSE PUBLIC LICENSE, NEITHER THE ECLIPSE FOUNDATION NOR ANY CONTRIBUTORS TO THE ECLIPSE PROGRAM SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE ECLIPSE PROGRAM, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any provisions provided by Infoblox relating to the Eclipse Program which differ from the above terms or the Eclipse Public License are offered by Infoblox alone and not by any other party.

The source code for the Eclipse Program is available from Infoblox as described in the open source introduction.

**Eclipse Public License - v 1.0**

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS ECLIPSE PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution `originates` from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.
"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must:

a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend
claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. The Eclipse Foundation is the initial Agreement Steward. The Eclipse Foundation may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

Related Links
* EPL in plain HTML
* The EPL on OSI's site
* CPL to EPL conversion

AOP Alliance (Java/J2EE AOP standards)

LICENSE: all the source code provided by AOP Alliance is Public Domain.

OpenJDK

GNU General Public License, version 2, with the Classpath Exception

The GNU General Public License (GPL) Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License

Copyright ©2019, Infoblox, Inc. All right reserved.
License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too. When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things. To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License.The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control
compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED
IN ACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

One line to give the program's name and a brief idea of what it does.

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License.Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

"CLASSPATH" EXCEPTION TO THE GPL

Certain source files distributed by Oracle America and/or its affiliates are subject to the following clarification and special exception to the GPL, but only where Oracle has expressly included in the particular source file's header the words "Oracle designates this particular file as subject to the "Classpath" exception as provided by Oracle in the LICENSE file that accompanied this code."

Linking this library statically or dynamically with other modules is making a combined work based on this library. Thus, the terms and conditions of the GNU General Public License cover the whole combination.

As a special exception, the copyright holders of this library give you permission to link this library with independent modules to produce an executable, regardless of the license terms of these independent modules, and to copy and distribute the resulting executable under terms of your choice, provided that you also meet, for each linked independent module, the terms and conditions of the license of that module.An independent module is a module which is not derived from or based on this library. If you modify this library, you may extend this exception to your version of the library, but you are not obligated to do so. If you do not wish to do so, delete this exception statement from your version.

TASM

Copyright (c) 2000-2005 INRIA, France Telecom All rights reserved.

Copyright ©2019, Infoblox, Inc.All right reserved.
3. Neither the name of the copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Distributed Computing Laboratory, Emory University

This software is released to the public domain, in the spirit of the original code written by Doug Lea. The code can be used for any purpose, modified, and redistributed without acknowledgment. No warranty is provided, either express or implied.

COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL)

Version 1.0

1. Definitions.
   1.1. Contributor means each individual or entity that creates or contributes to the creation of Modifications.
   1.2. Contributor Version means the combination of the Original Software, prior Modifications used by a Contributor (if any), and the Modifications made by that particular Contributor.
   1.3. Covered Software means (a) the Original Software, or (b) Modifications, or (c) the combination of files containing Original Software with files containing Modifications, in each case including portions thereof.
   1.4. Executable means the Covered Software in any form other than Source Code.
   1.5. Initial Developer means the individual or entity that first makes Original Software available under this License.
   1.6. Larger Work means a work which combines Covered Software or portions thereof with code not governed by the terms of this License.
   1.7. License means this document.
   1.8. Licensable means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.
   1.9. Modifications means the Source Code and Executable form of any of the following:
      A. Any file that results from an addition to, deletion from or modification of the contents of a file containing Original Software or previous Modifications;
      B. Any new file that contains any part of the Original Software or previous Modification; or
      C. Any new file that is contributed or otherwise made available under the terms of this License.
   1.10. Original Software means the Source Code and Executable form of computer software code that is originally released under this License.
   1.11. Patent Claims means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.
   1.12. Source Code means (a) the common form of computer software code in which

2. License Grants.
   2.1. The Initial Developer Grant.

Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, the Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license:

   (a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer, to use, reproduce, modify, display, perform, sublicense and distribute the Original Software (or portions thereof), with or without Modifications, and/or as part of a Larger Work; and

   (b) under Patent Claims infringed by the making, using or selling of Original Software, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Software (or portions thereof).
(c) The licenses granted in Sections 2.1(a) and (b) are effective on the date Initial Developer first distributes or otherwise makes the Original Software available to a third party under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: (1) for code that You delete from the Original Software, or (2) for infringements caused by: (i) the modification of the Original Software, or (ii) the combination of the Original Software with other software or devices.

2.2. Contributor Grant.

Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof), either on an unmodified basis, with other Modifications, as Covered Software and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: (1) Modifications made by that Contributor (or portions thereof); and (2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) The licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first distributes or otherwise makes the Modifications available to a third party.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: (1) for any code that Contributor has deleted from the Contributor Version; (2) for infringements caused by: (i) third party modifications of Contributor Version, or (ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or (3) under Patent Claims infringed by Covered Software in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Availability of Source Code.

Any Covered Software that You distribute or otherwise make available in Executable form must also be made available in Source Code form and that Source Code form must be distributed only under the terms of this License.

You must include a copy of this License with every copy of the Source Code form of the Covered Software You distribute or otherwise make available. You must inform recipients of any such Covered Software in Executable form as to how they can obtain such Covered Software in Source Code form in a reasonable manner on or through a medium customarily used for software exchange.

3.2. Modifications.

The Modifications that You create or to which You contribute are governed by the terms of this License. You represent that You believe Your Modifications are Your original creation(s) and/or You have sufficient rights to grant the rights conveyed by this License.

3.3. Required Notices.

You must include a notice in each of Your Modifications that identifies You as the Contributor of the Modification. You may not remove or alter any copyright, patent or trademark notices contained within the Covered Software, or any notices of licensing or any descriptive text giving attribution to any Contributor or the Initial Developer.

3.4. Application of Additional Terms.

You may not offer or impose any terms on any Covered Software in Source Code form that alters or restricts the applicable version of this License or the recipients rights hereunder. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, you may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear that any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.5. Distribution of Executable Versions.

You may distribute the Executable form of the Covered Software under the terms of this License or under the terms of a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable form does not attempt to limit or alter the recipients rights in the Source Code form from the rights set forth in this License. If You distribute the Covered Software in Executable form under a different license, You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.


You may create a Larger Work by combining Covered Software with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Software.

4. Versions of the License.

4.1. New Versions.
4.2. Effect of New Versions.

You may always continue to use, distribute or otherwise make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. If the Initial Developer includes a notice in the Original Software prohibiting it from being distributed or otherwise made available under any subsequent version of the License, You must distribute and make the Covered Software available under the terms of the License under which You originally received the Covered Software. Otherwise, You may also choose to use, distribute or otherwise make the Covered Software available under the terms of any subsequent version of the License published by the license steward.

4.3. Modified Versions.

When You are an Initial Developer and You want to create a new license for Your Original Software, You may create and use a modified version of this License if You: (a) rename the license and remove any references to the name of the license steward (except to note that the license differs from this License); and (b) otherwise make it clear that the license contains terms which differ from this License.

5. DISCLAIMER OF WARRANTY.

COVERED SOFTWARE IS PROVIDED UNDER THIS LICENSE ON AN AS IS BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED SOFTWARE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED SOFTWARE IS WITH YOU. SHOULD ANY COVERED SOFTWARE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED SOFTWARE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

6. TERMINATION.

6.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

6.2. If You assert a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You assert such claim is referred to as Participant) alleging that the Participant Software (meaning the Contributor Version where the Participant is a Contributor or the Original Software where the Participant is the Initial Developer) directly or indirectly infringes any patent, then any and all rights granted directly or indirectly to You by such Participant, the Initial Developer (if the Initial Developer is not the Participant) and all Contributors under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively and automatically at the expiration of such 60 day notice period, unless if within such 60 day period You withdraw Your claim with respect to the Participant Software against such Participant either unilaterally or pursuant to a written agreement with Participant.

6.3. In the event of termination under Sections 6.1 or 6.2 above, all end user licenses that have been validly granted by You or any distributor hereunder prior to termination (excluding licenses granted to You by any distributor) shall survive termination.

7. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED SOFTWARE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY NATURE INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL APPLY TO ALL LIABILITY OF THE LICENSEE UNDER THIS LICENSE, INCLUDING LIABILITY ARISING FROM THE PERFORMANCE OR NONPERFORMANCE OF THE LICENSED SOFTWARE.

8. U.S. GOVERNMENT END USERS.

The Covered Software is a commercial item, as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of commercial computer software (as that term is defined at 48 C.F.R. 252.227-7014(a)(1)) and commercial computer software documentation as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Software with only those rights set forth herein. This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFAR, or other clause or provision that addresses Government rights in computer software under this License.

9. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by the law of the jurisdiction specified in a notice contained within the Original Software (except to the extent applicable law, if any, provides otherwise), excluding such jurisdictions conflict-of-law provisions. Any litigation relating to this License shall be subject to the jurisdiction of the courts located in the jurisdiction and venue specified in a notice contained within the Original Software, with the losing party responsible for costs, including, without limitation, court costs and reasonable attorneys fees and expenses. The application of the United Nations Convention on Contracts for the
International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License. You agree that You alone are responsible for compliance with the United States export administration regulations (and the export control laws and regulation of any other countries) when You use, distribute or otherwise make available any Covered Software.

10. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

The FreeType Project LICENSE

2002-Apr-11

Copyright 1996-2002 by
David Turner, Robert Wilhelm, and Werner Lemberg

Introduction
============

The FreeType Project is distributed in several archive packages; some of them may contain, in addition to the FreeType font engine, various tools and contributions which rely on, or relate to, the FreeType Project.

This license applies to all files found in such packages, and which do not fall under their own explicit license. The license affects thus the FreeType font engine, the test programs, documentation and makefiles, at the very least.

This license was inspired by the BSD, Artistic, and IJG (Independent JPEG Group) licenses, which all encourage inclusion and use of free software in commercial and freeware products alike. As a consequence, its main points are that:

- We don't promise that this software works. However, we will be interested in any kind of bug reports. (‘as is’ distribution)
- You can use this software for whatever you want, in parts or full form, without having to pay us. (‘royalty-free’ usage)
- You may not pretend that you wrote this software. If you use it, or only parts of it, in a program, you must acknowledge somewhere in your documentation that you have used the FreeType code. (‘credits’)

We specifically permit and encourage the inclusion of this software, with or without modifications, in commercial products. We disclaim all warranties covering The FreeType Project and assume no liability related to The FreeType Project.

Finally, many people asked us for a preferred form for a credit/disclaimer to use in compliance with this license. We thus encourage you to use the following text:

```
* * *
Portions of this software are copyright © 1996-2002 The FreeType Project (www.freetype.org). All rights reserved.
```

Legal Terms
===========

0. Definitions
--------------

Throughout this license, the terms ‘package’, ‘FreeType Project’, and ‘FreeType archive’ refer to the set of files originally distributed by the authors (David Turner, Robert Wilhelm, and Werner Lemberg) as the ‘FreeType Project’, be they named as alpha, beta or final release.

‘You’ refers to the licensee, or person using the project, where ‘using’ is a generic term including compiling the project’s source code as well as linking it to form a ‘program’ or ‘executable’. This program is referred to as ‘a program using the FreeType engine’.

This license applies to all files distributed in the original FreeType Project, including all source code, binaries and documentation, unless otherwise stated in the file in its original, unmodified form as distributed in the original archive. If you are unsure whether or not a particular file is covered by this license, you must contact us to verify this.

The FreeType Project is copyright (C) 1996-2000 by David Turner, Robert Wilhelm, and Werner Lemberg. All rights reserved except as specified below.

1. No Warranty
--------------

THE FREE TYPE PROJECT IS PROVIDED ‘AS IS’ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL ANY OF THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY DAMAGES CAUSED BY THE USE OR THE INABILITY TO USE, OF THE FREE TYPE PROJECT.

2. Redistribution
--------------
This license grants a worldwide, royalty-free, perpetual and irrevocable right and license to use, execute, perform, compile, display, copy, create derivative works of, distribute and sublicense the FreeType Project (in both source and object code forms) and derivative works thereof for any purpose; and to authorize others to exercise some or all of the rights granted herein, subject to the following conditions:

- Redistribution of source code must retain this license file (`FTL.TXT') unaltered; any additions, deletions or changes to the original files must be clearly indicated in accompanying documentation. The copyright notices of the unaltered, original files must be preserved in all copies of source files.
- Redistribution in binary form must provide a disclaimer that states that the software is based in part of the work of the FreeType Team, in the distribution documentation. We also encourage you to put an URL to the FreeType web page in your documentation, though this isn't mandatory.

These conditions apply to any software derived from or based on the FreeType Project, not just the unmodified files. If you use our work, you must acknowledge us. However, no fee need be paid to us.

3. Advertising

Neither the FreeType authors and contributors nor you shall use the name of the other for commercial, advertising, or promotional purposes without specific prior written permission.

We suggest, but do not require, that you use one or more of the following phrases to refer to this software in your documentation or advertising materials: `FreeType Project', `FreeType Engine', `FreeType library', or `FreeType Distribution'.

As you have not signed this license, you are not required to accept it. However, as the FreeType Project is copyrighted material, only this license, or another one contracted with the authors, grants you the right to use, distribute, and modify it. Therefore, by using, distributing, or modifying the FreeType Project, you indicate that you understand and accept all the terms of this license.

4. Contacts

There are two mailing lists related to FreeType:

- freetype@freetype.org
  Discusses general use and applications of FreeType, as well as future and wanted additions to the library and distribution. If you are looking for support, start in this list if you haven't found anything to help you in the documentation.

- devel@freetype.org
  Discusses bugs, as well as engine internals, design issues, specific licenses, porting, etc.

- http://www.freetype.org
  Holds the current FreeType web page, which will allow you to download our latest development version and read online documentation.

You can also contact us individually at:

David Turner <david.turner@freetype.org>
Robert Wilhelm <robert.wilhelm@freetype.org>
Werner Lemberg <werner.lemberg@freetype.org>

The Independent JPEG Group’s JPEG software

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)
2. You can use this software for whatever you want. You don't have to pay us.
3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-1998, Thomas G. Lane. All Rights Reserved except as specified below.
Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, lconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software. (Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that

"The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated.GIF(sm) is a Service Mark property of CompuServe Incorporated."

Net-SNMP

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts. Up until 2001, the project was based at UC Davis, and the first part covers all code written during this time. From 2001 onwards, the project has been based at SourceForge, and Networks Associates Technology, Inc hold the copyright on behalf of the wider Net-SNMP community, covering all derivative work done since then. An additional copyright section has been added as Part 3 below also under a BSD license for the work contributed by Cambridge Broadband Ltd. to the project since 2001. An additional copyright section has been added as Part 4 below also under a BSD license for the work contributed by Sun Microsystems, Inc. to the project since 2003.

Code has been contributed to this project by many people over the years it has been in development, and a full list of contributors can be found in the README file under the THANKS section.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----


Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE
• Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

• Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2005, Sparta, Inc All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

• Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

• Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

• Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

• Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

• Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

• Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright ©2019, Infoblox, Inc.All right reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The PHP License, version 3.01

Copyright (c) 1999 - 2006 The PHP Group. All rights reserved. Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.

4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo".

5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes PHP software, freely available from <http://www.php.net/software/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project,

please see <http://www.php.net>.


INFO-ZIP

Copyright (c) 1990-2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:


This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions—including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP—must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases-including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.


MIT License

Copyright (c) 2010 Paul T. McGuire

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Ehcache

The open source Ehcache project is licensed under the Apache 2.0 License. The text of the license is available below:

Copyright 2003-2010 Terracotta, Inc.

Licensed under the Apache License, Version 2.0 (the "License");

you may not use this file except in compliance with the License.

You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.
Cybox

Copyright (c) 2015, The MITRE Corporation All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of The MITRE Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Dateutil

dateutil - Extensions to the standard Python datetime module.

Copyright (c) 2003-2011 - Gustavo Niemeyer <gustavo@niemeyer.net>
Copyright (c) 2012-2014 - Tomi Pievilainen <tomi.pievilainen@iki.fi>
Copyright (c) 2014- Yaron de Leeuw <me@jarondl.net>

All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Importlib

(No license included in the package, this is in the readme)

Purpose
=======

This package contains the code from importlib as found in Python 2.7. It is provided so that people who wish to use "importlib.import_module()" with a version of Python prior to 2.7 or in 3.0 have the function readily available. The code in no way deviates from what can be found in the Python 2.7 standard library.

For documentation, see the `importlib docs`_ for Python 2.7.

Libtaxii

Copyright (c) 2013, The MITRE Corporation All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of The MITRE Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Mixbox

Copyright (c) 2015, The MITRE Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of The MITRE Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Stix

Copyright (c) 2015, The MITRE Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of The MITRE Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PSF License Agreement for Python 2.6

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.
4. PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

Copyright ©2019, Infoblox, Inc. All right reserved.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

PSF License Agreement for Python 3.5.0

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 3.5.0 software in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 3.5.0 alone or in any derivative version, provided, however, that PSF’s License Agreement and PSF’s notice of copyright, i.e., “Copyright © 2001-2015 Python Software Foundation; All Rights Reserved” are retained in Python 3.5.0 alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on or incorporates Python 3.5.0 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 3.5.0.
4. PSF is making Python 3.5.0 available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 3.5.0 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 3.5.0 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 3.5.0, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python 3.5.0, Licensee agrees to be bound by the terms and conditions of this License Agreement.

GNU General Public License 2.0 for Suricata, Netfilter and IPTables

GNU General Public License
Version 2, June 1991 Copyright © 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, you need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of
it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification"). Each licensor is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange;
   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange;
   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or redistribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, modifying or distributing the Program or works based on it.

6. Each person redistributing the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients’ exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in
reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) <year> name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items–whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General
Public License instead of this License.

LibYAML

Copyright (c) 2006 Kirill Simonov
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The MIT License for Jansson

Copyright <YEAR> <COPYRIGHT HOLDER>
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

PCRE - Perl Compatible Regular Expressions

PCRE2 LICENCE
-------------
PCRE2 is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.
Release 10 of PCRE2 is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE2, supplied in the "doc" directory, is distributed under the same terms as the software itself. The data in the testdata directory is not copyrighted and is in the public domain.
The basic library functions are written in C and are freestanding. Also included in the distribution is a just-in-time compiler that can be used to optimize pattern matching. This is an optional feature that can be omitted when the library is built.

THE BASIC LIBRARY FUNCTIONS
----------------------------
Written by: Philip Hazel Email local part: ph10
Email domain: cam.ac.uk
Copyright (c) 1997-2016 University of Cambridge All rights reserved.

PCRE2 JUST-IN-TIME COMPILATION SUPPORT
--------------------------------------
Written by: Zoltan Herczeg Email local part: hzmester
Email domain: freemail.hu Copyright(c) 2010-2016 Zoltan Herczeg All rights reserved.

STACK-LESS JUST-IN-TIME COMPILER
--------------------------------
Written by: Zoltan Herczeg Email local part: hzmester
Email domain: freemail.hu Copyright(c) 2009-2016 Zoltan Herczeg All rights reserved.

THE "BSD" LICENCE
-----------------
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the names of any contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
Appendix I Configuration Requiring Service Restart

This document includes a list of objects that require service restart after you make configuration changes to them. For more information about restarting services, see Restarting Services.

Table H.1 Object Changes that Require Service Restart

<table>
<thead>
<tr>
<th>Object</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid Security Properties</td>
<td>DNS</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Member Security Properties</td>
<td>DNS</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Authoritative Zone</td>
<td>DNS</td>
<td>Insert, update, delete</td>
<td>If the &quot;Restart if needed&quot; option is enabled, restart is triggered immediately.</td>
</tr>
<tr>
<td>DNS Traffic Control Monitor</td>
<td>DNS</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Network Container</td>
<td>DHCP</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>Shared Network</td>
<td>DHCP</td>
<td>Insert, delete</td>
<td></td>
</tr>
<tr>
<td>Blacklist Rule</td>
<td>DNS</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>Bulk Host</td>
<td>DNS</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>Convert Lease</td>
<td>DHCP</td>
<td>Convert</td>
<td></td>
</tr>
<tr>
<td>Convert IPv6 Lease</td>
<td>DHCP</td>
<td>Convert</td>
<td></td>
</tr>
<tr>
<td>Grid DHCP Failover Association</td>
<td>DHCP</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>DHCP Fingerprint Filter</td>
<td>DHCP</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Grid DHCP MAC Filter</td>
<td>DHCP</td>
<td>Update, delete</td>
<td></td>
</tr>
<tr>
<td>DHCP Range</td>
<td>DHCP</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>DNS64 synthesis group</td>
<td>DNS</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>NS Group and Authoritative zone</td>
<td>DNS</td>
<td>Changing list of secondaries</td>
<td></td>
</tr>
<tr>
<td>Grid DNS Properties</td>
<td>DNS</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Member DNS Properties</td>
<td>DNS</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>RolloverKey</td>
<td>DNS</td>
<td>Rollover</td>
<td></td>
</tr>
<tr>
<td>DNSSEC Sign Zone</td>
<td>DNS</td>
<td>Sign</td>
<td></td>
</tr>
<tr>
<td>Fixed Address</td>
<td>DHCP</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>Forward Zone</td>
<td>DNS</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>Grid DHCP Properties</td>
<td>DHCP</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Host Record</td>
<td>DNS</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>Host Name Rewrite Policy</td>
<td>DHCP</td>
<td>Insert, update</td>
<td></td>
</tr>
<tr>
<td>DNS Traffic Control Load Balanced Domain Name</td>
<td>DNS</td>
<td>Insert, update, delete, restore</td>
<td></td>
</tr>
<tr>
<td>DNS Traffic Control Pool</td>
<td>DNS</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>DNS Traffic Control Server</td>
<td>DNS</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>DNS Traffic Control Topology Rule</td>
<td>DNS</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>IPv6 DHCP Range</td>
<td>DHCP</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>IPv6 Fixed Address</td>
<td>DHCP</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>IPv6 Network</td>
<td>DHCP</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>IPv6 Option Space</td>
<td>DHCP</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>IPv6 Shared Network</td>
<td>DHCP</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Member DHCP Properties</td>
<td>DHCP</td>
<td>Insert, update</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Type</td>
<td>Action</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>NAC Filter</td>
<td>DHCP</td>
<td>Update, delete</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>DHCP</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>Network View</td>
<td>DHCP</td>
<td>Update, delete</td>
<td></td>
</tr>
<tr>
<td>NS Group</td>
<td>DNS</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>NXDOMAIN Rule</td>
<td>DNS</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>DHCP Range Option Filter</td>
<td>DHCP</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>DHCP Option Space</td>
<td>DHCP</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Order DHCP Ranges</td>
<td>DHCP</td>
<td>Changing order of DHCP ranges</td>
<td></td>
</tr>
<tr>
<td>DHCP Relay Agent Filter</td>
<td>DHCP</td>
<td>Update, delete</td>
<td></td>
</tr>
<tr>
<td>Resize Network</td>
<td>DHCP</td>
<td>Resize</td>
<td>Accessible from the IPAM tab</td>
</tr>
<tr>
<td>Response Policy Zone</td>
<td>DNS</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Roaming Host</td>
<td>DHCP</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>Ruleset</td>
<td>DNS</td>
<td>Update, delete</td>
<td></td>
</tr>
<tr>
<td>IPv4/IPv6 Shared Network</td>
<td>DHCP</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Split Network</td>
<td>DHCP</td>
<td>Split</td>
<td>Accessible from the IPAM tab</td>
</tr>
<tr>
<td>Join Network</td>
<td>DHCP</td>
<td>Join</td>
<td>Accessible from the IPAM tab</td>
</tr>
<tr>
<td>Stub Zone</td>
<td>DNS</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>DNS</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>Import Topology Database</td>
<td>DNS</td>
<td>Import</td>
<td></td>
</tr>
<tr>
<td>Named ACL</td>
<td>DNS</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Grid Properties</td>
<td>DNS</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Member Properties</td>
<td>DNS</td>
<td>Insert, update, delete</td>
<td></td>
</tr>
<tr>
<td>RADIUS Authentication Service</td>
<td>DHCP</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Grid Reporting Properties</td>
<td>DNS, DHCP</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Reporting Ip Block Group</td>
<td>DNS</td>
<td>Update, delete</td>
<td></td>
</tr>
<tr>
<td>Reporting Member Properties</td>
<td>DNS, DHCP</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>HSM SafeNet Group</td>
<td>DNS</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>License</td>
<td>DNS</td>
<td>Delete</td>
<td>Restarts for QRD, RPZ, MSMGMT and REPORTING licenses.</td>
</tr>
</tbody>
</table>